Aker Firewall

Version 12/20/2012

AKER
www.aker.com.br

Index

Index ... *2*

Image Index ... *9*

1. Introduction ... 18

1.1. How this manual is arranged ... 18

1.2. Text Interface and Remote Interface ... 19

1.3. The Firewall ... 19

1.4. System Copyrights ... 21

2. Installing Aker Firewall ... 23

2.1. Hardware and software requirements ... 23

2.2. Remote Interface installation ... 24

2.3. Aker Firewall Installation ... 31

2.4. Firewall Aker – Installation Program ... 34

2.5. Remote users administration module and including users ... 36

3. Using Aker Control Center ... 39

3.1. What is Aker Firewall remote administration? ... 39

3.2. Starting remote interface ... 41

3.3. Ending remote administration ... 59

3.4. Changing user passwords ... 60

3.5. Visualizing session information ... 62

3.6. Using Remote Interface tools ... 63

3.7. Activation Keys ... 64

3.8. Saving configurations (backup) ... 65

3.9. Restore configurations ... 68

3.10. Restarting the Firewall ... 71

3.11. Updates ... 72

3.12. Automatic Update Module – Aker Update System (AUS) ... 77

3.13. DNS Look up ... 81

3.14. Filtering Rules Simulation ... 83

3.15. Reports ... 86

3.16. *Entity Search* 88
3.17. *Alarm Window* 92
3.18. *Network View* 94
3.19. *System statistics*....................95
3.20. *Using the Packet Sniffer window*....................98
3.21. *Viewing the State of External Agents* 102
3.22. *Using the Configurations Checker*....................104
3.23. *Diagnosis* 108

4. Administering Firewall users 115

4.1. *Administrator Users*....................115
4.2. *Using the text interface*....................128

5. Configuring the system parameters 139

5.1. *Using the Remote Interface*....................139
5.2. *Using the text interface*....................154

6. Registering Entities....................159

6.1. *Planning installation* 159
6.2. *Registering entities using the Remote Interface* 163
6.3. *Using the text interface*....................200
6.4. *Using the entity wizard* 204

7. Stateful Inspection 212

7.1. *Planning the installation* 212
7.2. *Editing a list of rules using the Remote Interface* 218
7.3. *Working with the filtering Polices*....................226
7.4. *Using the text interface*....................228
7.5. *Using the Filtering rules wizard.* 231
7.6. *Using the Pipes rules* 243

8. Configuring the address translation....................246

8.1. *Planning installation* 246
8.2. *Using the Text Interface* 270
8.3. *Using the NAT configuration wizard* 274

9. Creating encryption channel 283

9.1. Nat Traversal (NAT-T)...283

9.2. Planning installation 284

9.3. Using the Text Interface 306

10. Configuring Client-Firewall secure channels 314

10.1. Planning installation 314

10.2. Aker Secure Roaming 315

10.3. L2TP...321

10.4. PPTP...330

10.5. IPSEC Client 352

10.6. VPN – SSL 368

11. Configuring Client-Firewall encryption...382

11.1. Editing the SSL context parameters 383

11.2. Configuring Proxy SSL rules 387

12. Integration of Firewall modules...389

12.1. The flow of packets on Aker Firewall..389

12.2. Integrating the filter with the address translation 391

12.3. Integrating the filter with the network address translation..............................392

13. Configuring the security 394

13.1. Protection against SYN Flood 394

13.2. Using the Remote Interface for protection against SYN Flood 396

13.3. Flood Protection 398

13.4. Using the Remote Interface for Flood protection..399

13.5. Anti-Spoofing Security..401

13.6. Using the Text Interface – Syn Flood 402

13.7. Using the Remote Interface for Anti-Spoofing 404

13.8. Using the text interface – Flood Protection...406

13.9. Using the text interface – Anti Spoofing 407

13.10. Block by excessive invalid logins attempts 408

14. Configuring the system actions 410

14.1. Using the remote interface 410
14.2. Using the text interface..415

15. Viewing the system log 421
15.1. Using the Remote Interface...422
15.2. Format and meaning of the fields of log records 432
15.3. Using the text interface..437

16. Viewing system events...440
16.1. Using the Remote Interface...440
16.2. Format and meaning of messages and events fields 447
16.3. Using the Text Interface 448

17. Viewing statistics..451
17.1. Using the Remote Interface...452
17.2. Using the Text Interface 457

18. Viewing and removing connections...462
18.1. Using the Remote Interface...463
18.2. Using the Text Interface 468

19. Using the Reports generator 472
19.1. Accessing reports...472
19.2. Configuring Reports 473
19.3. List of available reports 479

20. Logs and events scheduled exports 482
20.1. Accessing the logs and events scheduled exports 482
20.2. Configuring the logs and events scheduled exports 483

21. Working with proxies..488
21.1. Planning the installation 488
21.2. Installing the authentication agent on Unix Platforms...494
21.3. Installing the authentication agent on Windows Server^{tm} 496
21.4. Configuring authentication agent for Windows Server^{tm} 497

22. Configuring the authentication parameters 502

22.1. Using the remote Interface 502
22.2. Using the text interface 518

23. Users access profile 521
23.1. Planning the installation 521
23.2. Registering access profiles 522
23.3. Rules 526
23.4. SOCKS rules 527
23.5. General 528
23.6. FTP and GOPHER 529
23.7. HTTP/HTTPS 533
23.8. Secure Roaming 542
23.9. VPN SSL (Proxy SSL) 545
23.10. MSN Messenger 548
23.11. Application filtering 550
23.12. Associating users with access profile 552

24. User authentication 558
24.1. Viewing and removing users connected to the Firewall 558
24.2. Using the Text Interface 561

25. Configuring the SMTP proxy 564
25.1. Editing parameters of an SMTP context 566

26. Configuring the Telnet proxy 589
26.1. Editing the parameters of a telnet context 589

27. Configuring the FTP proxy 594
27.1. Editing the parameters of a FTP context 595

28. Configuring the POP3 proxy 599
28.1. Editing parameters of a POP3 context 600

29. Using Quotas 606
29.1. Editing parameters of Quota usage 606

30. Configuring Web filter 612

30.1. Planning the installation 612
30.2. Editing the Web Filter parameters..615
30.3. Editing Web session parameters..652

31. Configuring Socks proxy 655
31.1. Planning the installation 655
31.2. Editing the parameters of SOCKS proxy 656

32. Configuring the RPC proxy and DCE-RPC proxy..659
32.1. Editing the parameters of a RPC context 661
Editing the parameters of a DCE-RPC context 663

33. Configuring the MSN proxy..666
33.1. Planning the installation 666
33.2. Editing the MSN proxy parameters..667

34. Configuring the application filtering 673
34.1. Planning the installation 673
34.2. Creating Application filtering rules..673
34.3. Creating application filters 678

35. Configuring the IDS/IPS 683
35.1. Accessing the IPS/IDS 683
35.2. View blocked IPs..693
35.3. Installing IDS External Plugin on Windows..696
35.4. Using the Text Interface – Portscan 702
35.5. Using the Text Interface – External IDS 703

36. TCP/IP settings..706
36.1. TCP/IP settings 706
36.2. DHCP 707
36.3. DNS..711
36.3.1. Network interfaces 712
36.4. Routing..717
36.4.1. Global 719
36.4.2. Dynamic..721

36.4.3. Advanced 729

36.5. Using the Text Interface for Activation Keys 735

36.6. Using the Text Interface for TCP/IP configuration 735

36.7. Using the text interface for Wireless configuration 744

36.8. Using the Text Interface for DDNS configuration...................................748

36.9. 3G link configuration...750

36.10 Link aggregation 750

37. Configuring the firewall in Cluster 755

37.1. Planning the installation 755

37.2. Cluster configuration 757

37.3. Cluster statistics 763

37.4. Configuring the cooperative cluster 765

37.5. Using the Text Interface 776

38. System files 780

38.1. System files 780

39. Aker Firewall Box 785

40. Aker Web Content Analyzer – AWCA 790

40.1. Introduction 790

40.2. Prerequisite 791

40.3. Installing Aker Web Content Analyzer 791

40.4. Installation on a windows platform..792

40.5. Installation on a Linux platform (Fedora) 799

40.6. AWCA configuration 805

40.7. Database management 806

40.8. Categories 811

40.9. URL test 821

41. Aker Spam Meter – ASM 825

41.1. Introduction 825

41.2. Presenting ASM (Aker Spam Meter) 826

41.3. How does the classification work...826

41.4. Aker Control Center 827
41.5. Databases 829
41.6. E-mail classification 834
41.7. Filter settings 837
41.8. Score graph 840
41.9. Plugins 841

42. Aker Antivirus Module – AKAV 843
42.1. Introduction 843
42.2. Introducing the appliance 844
42.3. Main features 845
42.4. Aker Antivirus Module 846
42.5. Configuring Aker Antivirus Modulo 846
42.6. Settings 848
42.7. Engine information 850
42.8. Update management 851

43. Appendix B – Copyrights e Disclaimers 856

Image Index

Image 1 – Installation language 24
Image 2 – Aker Control Center 2 Installation (welcome message) 25
Image 3 – Software license agreement 26
Image 4 – User information 27
Image 5 – Destination Folder 28
Image 6 – Installation inside a specific folder 29
Image 7 – Ready to install application 29
Image 8 – Installation Bar Status. 30
Image 9 – Successful installation message. 31
Image 10 – Select the product to be installed or configured. 33
Image 11 – Read the following text carefully and confirm installation. 33
Image 12 – Select which disk the product will be installed, ...34
Image 14 – Accessing Aker Control Center 2. 41
Image 15 – Access window: Options menu. 42
Image 16 – Idle session time. 43

Image 17 – Hide rules. 43
Image 18 – Disable questions. 43
Image 19 – Choose the language you wish to access Aker Control Center. 44
Image 20 – Aker Control Center background color 44
Image 21 – Horizontal format. 44
Image 22 – Vertical format. 45
Image 23 – Diagonal format. 45
Image 24 – Automatic horizontal. 45
Image 25 – Automatic vertical format. 45
Image 26 – Select color. 46
Image 27 – Button: Default. 46
Image 28 – Exit warning. 46
Image 29 – Windows menu. 47
Image 30 – Access Window: remote devices. 47
Image 31-Access Window: entities. 48
Image 32-Access Window: windows. 48
Image 33 – Automatic Update Configuration. 48
Image 34 – Update Notifier 49
Image 35-Update Installation Notifier. 49
Image 36 – Updates(s) ready. 50
Image – 37 Information on the topic (About) 50
Image 38-Access Window: Aker Firewall. 51
Image 40 – Button: Create a new remote device. 52
Image 43 – Icon used to load files. 55
Image 44 – Icon used to show certificate information. 55
Image 45 – Authentication types (user, domain and password) to edit Remote Device. 56
Image 46 – Connect Button. 57
Image 49 – Button: Exit from this program. 59
Image 54 – Button: Load / Show license. 64
Image 56 – Button: Save backup of selected item. 65
Image 57 – Personalized configurations and products training base downloads. 66
Image 58 – Backup Log information. 66
Image 59 – File selection screen to save configurations. 67
Image 60 – Save backup automatically. 68
Image 62- Button: Loads file backups. 69
Image 63 – File selection to load configuration data. 69
Image 64 – Antivirus module backup restore. 70
Image 65 – Aker Spam Meter backup restore. 70
Image 66 – Web Content Analyzer backup restore. 71
Image 68 – Button: Updates. 72
Image 70 – Button: Load update file. 74
Image 71 – Selecting the file to be updated /corrected. 75

Image 72 – Apply patch or hotfix...75
Image 73 – Apply rollback..75
Image 75 – Accessing Aker Firewall 77
Image 76 – Notification of available updates on Aker Update System......................77
Image 77 – Visualizing available updates through Aker Update System. 78
Image 78 – Accessing Aker Firewall 79
Image 79 – Accessing Aker Update System window 79
Image 80 – Accessing Aker Firewall 80
Image 81 – Help menu...80
Image 83 – Reverse DNS 82
Image 84 – Access window to Filtering Rules Simulation...83
Image 85 – Filtering Rules Simulation (packet origin, date, time and masks)...........84
Image 87 – Access window: Report...86
Image 88 – Firewall configuration Report. 87
Image 90 – Entity Search (searches for an entity with IP or name and last results). 89
Image 91 – Entity Search (Services, protocol and last results).................................90
Image 92 – Entity Search (Rules, entities and last results)......................................91
Image 94 – Alarm Window (Description)...93
Image 95 – Access window: Network view. 94
Image 99 – System statistics report...98
Image 100 – Window access: Packet Sniffer..99
Image 101 – Packet Sniffer (Sniffer 1) 100
Image 103 – External Agents (name, type and status). 103
Image 105 – Configurations checker 106
Image 106 – Access Window: Diagnosis. 108
Image 107 –Diagnosis Window: All...109
Image 108 – Diagnosis Window: Ping 110
Image 109 – Diagnosis Window: Traceroute. 111
Image 110 – Diagnosis Window (Netstat tab)...112
Image 111 – Diagnosis Window (Nslookup tab) 113
Image 116 – Import certificate. 124
Image 117 – Certificate (imported)...124
Image 118 – Export certificate 125
Image 119 – Certificate (exported)...126
Image 120 – Certificate Details 126
Image 121 – Server choices option...128
Image 124 – Running the program to delete users...131
Image 125 – Running the program to alter a user’s password................................132
Image 127 – The program compression to show the user file compression. 134
Image 129 – Aker Configuration Manager setup (Enabled Firewall).........................136
Image 130 – Aker Configuration Manager Setup edition (Disable, modify return). .137
Image 132 – Configuration parameters (Global Tab)..141
Image 134 – Configuration parameters: Security tab 146

Image 136 –Configuration parameters: Monitoring tab 151
Image 138 – Entities window (Aker Firewall) 163
Image 139 – F5 button on your keyboard. 163
Image 140 – Entities: Aker Firewall Instance. 164
Image 143 – Networks adding and editing..168
Image 149 Category List adding and editing..175
Image 152 – External agents adding and editing. 178
Image 155 – Pseudo Group definition to users that authenticate themselves through the certification authority. 183
Image 157 – External agent: *Content Analyzer* registration. 184
Image 167 – File types list 196
Image 177 – Remote Devices (Access to rules configuration window)...................218
Image 179 – Menu with entities options regarding to the chosen field. 220
Image 180 – Verifying rules *icons*. 223
Image 182 – Filtering rules (Example of pipe 10Mb – ADSL). 224
Image 189 – Filtering rules wizard 231
Image 196 – Firewall configuration 238
Image 197 – Server Registration 239
Image 199 – Select the location where the DMZ will be available 241
Image 201 – *Filtering rules wizard* closing notice 243
Image 203 – 1st example of Aker Firewall configuration (*linking departments*) 251
Image 205 – 3rd Example of Aker Firewall configuration (*setting up the address translation rules*) 255
Image 207 – *Address Translation* configuration window (NAT). 257
Image 210 – Adding NAT rules windows. 261
Image 211 – *Weight* configuration window. 263
....267
Image 217 – Mounting NAT rules (Phase 2)..269
Image 223 – Choose the IP address used by external host, which will be used in the server. 279
Image 226 – Configuration of a Secure Channel Firewall-firewall to a sub network. 293
Image 227 – Secure channel between networks. 295
Image 229 – IPSEC certificates window. 297
Image 234 – Firewall-firewall options menu. 301
Image 241 – Security Roaming standard configuration. 316
Image 248 – Pop-up menu. 325
Image 252 – Configuring the L2TP client (User name and password used to authenticate the VPN client in Aker Firewall). 328
Image 255 – Pop-up menu. 333
Image 259 – VPN user name and password configuration window on Microsoft Windows®...337
Image 269 – Specifying connections conditions – Encryption. 348

Image 271 – Policy configuration method. 350
Image 273 – VPN clients (IPSEC) 353
Image 281 – Pop-up menu. 354
Image 282 – Pop-up menu. 356
Image 275 – Recommended configuration for encryption clients (X.509)...............359
Image 283 – VPN configuration with certificate...365
Image 285 – VPN configuration (Authentication Remote Identity) 366
Image 286 – VPN configuration (Authentication – Authentication Method).............367
Image 290 – Aker Authentication Agent wizard welcome screen. 373
Image 291 – License agreement...374
Image 292 – Destination folder. 375
Image 293 – Installing the program...376
Image 294 – Installation status bar. 377
Image 295 –Aker Authentication Agent installation has been completed................378
Image 307 – Access window: Anti-Spoofing. 404
Image 314 – access window (log)..422
Image 316 – *Firewall Log Filter* icon. 423
Image 317 – *Interrupt firewall search* icon. 423
Image 318 – *Export log* icon. 423
Image 319 – *Erase firewall log* icon. 423
Image 320 – *Reverse resolution of IP* icon 423
Image 321 – *Log screen refresh* icon..423
Image 322 – *Log update time* icon..424
Image 323 – *Go through log* icon..424
Image 324 – *Expand log messages* icon. 424
Image 325 – Log filter window. 425
Image 330 – Access window: Events...441
Image 333 – Description of events..445
Image 336 – Statistics rules...453
Image 339 – Button: Plot. 455
Image 340 – Button: List. 455
Image 341 – Button: remove...456
Image 342 –View statistics – Plot. 456
Image 343 – Button: save statistics. 457
Image 358 – Logs and events scheduled exports – Daily.......................................483
Image 360 – Logs and events scheduled export configuration – Publish Method. .485
Image 363 – Basic operation of a transparent proxy...490
Image 372 – Access authentication: Choosing a profile. 505
Image 374 – Access authentication: Adding entities..508
Image 376 – Access authentication: Method 1. 509
Image 383 – Local authentication – Create or delete groups...................................514
Image 388 – Profiles – Aker Firewall. 523
Image 391 – Profile: Socks. 527

Image 393 – Profiles: FTP and Gopher. 529
Image 396 – General: HTTP and HTTPS. 533
Image 399 – Toolbar (insert or disable) 536
Image 402 – Profiles: Security Roaming. 542
Image 403 – Profiles: Security Roaming (Address pool)...544
Image 405 – Direct connection: SSL Reverse Proxy. 546
Image 418 – Connected users (host, name, domain, profile, start, TPC and the number of logged users.) 559
Image 422 – Service: relay. 568
Image 438 – Services: FTP context configuration window.......................................595
Image 441 – Option menu. 601
Image 446 – Connection (Internet, Intranet, firewall and DMZ) 613
Image 451 – Web Filter; File types. 622
Image 454 – Certificate diagram. 629
Image 456 – Firefox certificate error. 632
Image 464 – CA certificate (Details) 640
Image 480 – Socks users authentication 656
Image 484 – Configuration of a DCE-RPC context. 663
Image 493 – Application filtering – Application filtering rules. 675
Image 496 – Application Filters..679
Image 514 – IDS configuration – events 701
Image 516 – Access window: DHCP. 707
Image 518 – DHCP relay among en. 709
Image 519 – Internal DHCP server. 710
Image 520 – Access window: DNS. 711
Image 522 – Access window: Network interfaces. 713
Image 523 – Access window: Network interfaces. 713
Image 524 – IP address configuration menu. 714
Image 527 – Access window: Routing 717
Image 528 – Routing window..718
Image 531 – Routing- Dynamic (RIP) 725
Image 532 – Routing- Dynamic (OSPF) 727
Image 533 – Routing – Advanced..729
Image 540 – Network Interfaces configuration module. 735
Image 541 – Interface configuration..736
Image 545 – Interface configuration..740
Image 546 – Static routes configuration...741
Image 556 – Cluster configuration – Global Information 760
Image 557 – Cluster configuration: Add Member..762
Image 558 – Access window: Cluster statistics. 763
Image 560 – Cluster statistic: Graphic 765
Image 561 – Access window: Cluster configuration. 766
Image 562 – Create Cluster. 766

Image 563 – Filling out the fields to create a cluster. 767
Image 564 – Example 768
Image 566 – Disconnecting message 769
Image 567 – Cooperative Cluster 770
Image 568 – Firewall Reboot message........771
Image 569 – Cluster Configuration 771
Image 570 – Choosing the mode 772
Image 571 – Adding entities. 773
Image 572 – Accessing the Text Interface 774
Image 573 – Registering MAC 774
Image 574 – Created cooperative cluster 775
Image 575 – Showing the interface configuration. 777
Image 576 – Web Content Analyzer diagram of operation. 790
Image 584 – Linux Installation: Unzipping. 799
Image 585 – Linux Installation: Installing AWCA. 800
Image 586 – License agreement........801
Image 589 – Setting user name and password........803
Image 591 – Aker Web Content Analyzer 805
Image 592 – Access window: Database management 806
Image 594 – Database management: General tab. 808
Image 600 – Icon button. 813
Image 601 – Choosing the category icon........814
Image 603 – Expression list creation. 815
Image 606 – Search button........817
Image 608 – Import file. 819
Image 609 – URL test 821
Image 610 – URL test. 822
Image 612 – Aker Spam Meter: Diagram of operation........827
Image 613 – Access window: Spam Meter. 828
Image 614 – Spam Meter menu........828
Image 615 – Access window: Databases. 829
Image 616 – Databases window. 830
Image 618 – Buttons: Save Backup and Restore Backup. 831
Image 619 – buttons: Refresh, recalculate and delete........832
Image 620 – Parameters. 833
Image 621 – Parâmetros: usando proxy. 834
Image 622 – Access window: E-mail classification. 835
Image 624 – Load an e-mail file........836
Image 625 – Access window: Filter settings. 837
Image 626 – Saved messages for training........837
Image 627 – Advanced Filter Settings. 838
Image 628 – Default button........839
Image 629 – Refresh button. 839

Image 630 – Score Graph..840
Image 631 – Score graph. 841
Image 633 – Aker Antivirus Module: Diagram of operation. 845
Image 635 – Diagram of operation 3...846
Image 636 – Antivirus 847
Image 637 – Aker Antivirus..848
Image 638 – Advanced Settings. 849
Image 640 – Update management...851
Image 641 – Update management (Proxy configuration)...852
Image 642 – Update management (Virus database Update)...................................853

Introduction

1. Introduction

Welcome to Aker Firewall User's Manual.

During the next chapters you will learn how to configure this powerful appliance of network protection. This introduction describes how this manual is organized and simplifies your reading, making it the most enjoyable possible.

1.1. How this manual is arranged

This manual is organized in a variety of chapters. Each chapter refers to one aspect of the product's setup as well as all the relevant information regarding the aspect discussed.

Each chapter starts off with a theoretical introduction to the topic in focus followed by specific aspects regarding Aker Firewall's configuration. Along with this theoretical introduction, some models feature practical usage examples of the service to be configured, in hypothetical situations, nevertheless, very close to reality. We aim at making your understanding the many configuration variables the simplest possible.

It is recommended that this manual be completely read, at least once, in its presented order. Subsequently, if necessary, it can and should be used as a reference source (to aid you through this manual, chapters have been organized into topics with immediate access on the main index, favoring the location of the desired information).

Throughout this manual, you will come across the symbol followed by a sentence in red. This means this specific sentence is a very important observation and it shall be totally understood before further reading on the chapter.

1.2. Text Interface and Remote Interface

Aker Firewall features two distinct interfaces for configuration: Remote Interface and a Text Interface.

- **Remote Interface:** The Remote Interface is called *remote* because it allows remote administration of Aker Firewall from anywhere in the world through the internet. This administration happens through a secured channel between interface and firewall, with a strong authentication scheme and encryption, in a way that it generates total security.

  The Remote Interface is of extreme intuitive use and is available for Windows and Linux platforms.

- **Text Interface:** The Text Interface has been fully oriented towards the Command Lines running on computers where the firewall is installed. Its basic objective is to allow automation of Aker Firewall administration tasks (through the creation of *scripts*) as well as the interaction of any script written by the administrator using the Firewall.

  Practically every variable which can be configured through the Remote Interface may also be configured through the text interface.

  Since both interfaces deal with the same variables, their functionality, their values as well as comments are applied to both graphic and text interfaces. Due to this, topics related to the Text Interface are normally short and limited to focusing on operation. In case of doubts regarding any parameters, resort to the explanation of that topic related to the Remote Interface.

The simultaneous use of many Remote Interfaces for the same Firewall is not possible.

1.3. The Firewall

As Internet evolves, application environments in router levels have become dynamic environments that constantly offer new protocols, services and applications. Routers and proxies are not enough and cannot ensure security to the wide array of Internet applications, let alone fulfill new business needs or high bandwidth and network security requirements. Faced with needs that organizations have to protect their networks, Aker has developed **Aker Firewall**.

Security surrounding networks is built by a set of programs and techniques aiming at liberating or blocking services within an Internet connected network in a controlled way. Being the Firewall the most important part of a security program, it is wise to remember the pertinence of using tools that aid the detection of breaches and vulnerabilities in the operational systems used within a network, as well as the use of programs that identify intruders and virtual attacks. It is also important to be aware of what measures will be taken in case of violation or shut down of an important service.

1.4. System Copyrights

- Copyright (c) 1997-2003 Aker Security Solutions;
- Uses the SSL library written by Eric Young (cay@mincon.oz.au). Copyright © 1995 Eric Young;
- Uses the AES algorithm implemented by Dr. B. R. Gladman (brg@gladman.uk.net);
- Uses the MD5 algorithm MD5 obtained from RFC 1321. Copyright © 1991-2 RSA Data Security, Inc;
- Uses the CMU SNMP library. Copyright© 1997 Carnegie Mellon University;
- Uses the Zlib compression library. Copyright © 1995-1998 Jean-loup Gailly and Mark Adler;
- Uses the QWT library written by Josef Wilgen. Copyright © 1997;
- Includes software developed by the University of California, Berkeley and their collaborators;
- Includes software developed by Luigi Rizzo, Universita di Pisa Portions Copyright 2000 Akamba Corp;
- Includes software developed by Niklas Hallqvist, Angelos D. Keromytis and Haan Olsson;
- Includes software developed by Ericsson Radio Systems.

Installing Aker Firewall

2. Installing Aker Firewall

This chapter will show how to install Aker Firewall, its software and Firewall installation requirements.

2.1. Hardware and software requirements

Firewall requirements

Aker Firewall runs on its own operational system, on Intel or any other compatible platforms.

To Aker Firewall execute all hardware components in a satisfactory manner, the following configurations are necessary:

- Intel or compatible Computer with 500 MHz or superior;

To use a link with a high transfer rate or use encryption on a link with relative high speed, we recommend the use of a more powerful computer.

- 512 Mbytes RAM memory;

For a better use of proxy and encryption services, the use of memory equal to or greater than 512 Mbytes is necessary.

- 20 Gbytes of disk space;

To store system logs for a longer period of time we recommend the use of a larger disk.

- CD-ROM drive or USB pen drive, screen, mouse and keyboard;

This is only necessary during the installation process or in case of Remote Interface being used from the console; however it is highly recommended in all cases.

- Network Interface Card(s).

There is no maximum number of NICs that can be placed in the Firewall. The only existing limitations are hardware limitations themselves. If a greater number of network interfaces is needed, NICs with more than one output on the same interface may be chosen.

Remote Interface requirements

Aker Firewall Remote Interface administration runs on Windows, Linux, Intel as well as other compatible platforms.

To make Aker Remote Interface (Control Center) run in a satisfactory way, hardware components should have the following configurations:

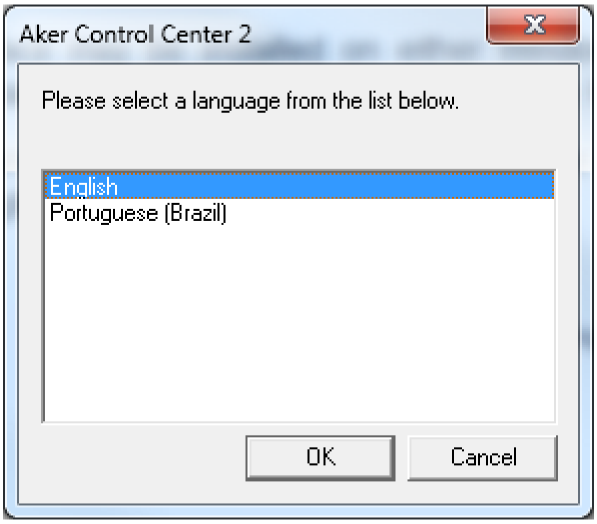
- Intel or compatible Computer with 500 MHz or superior;
- 256 Mbytes RAM memory;
- 2 Gbytes free disk space;
- Monitor;
- Mouse;
- Keyboard;
- Network Interface Card.

All hardware components shall be supported by the operational system on which the interface will be installed.

2.2. Remote Interface installation

The remote interface may be installed on either Windows or Linux platforms. Download and install Aker Control Center at: http://www.aker.com.br

Select the chosen language under which installation should be performed (Portuguese or English) and click the ***"OK"*** button.



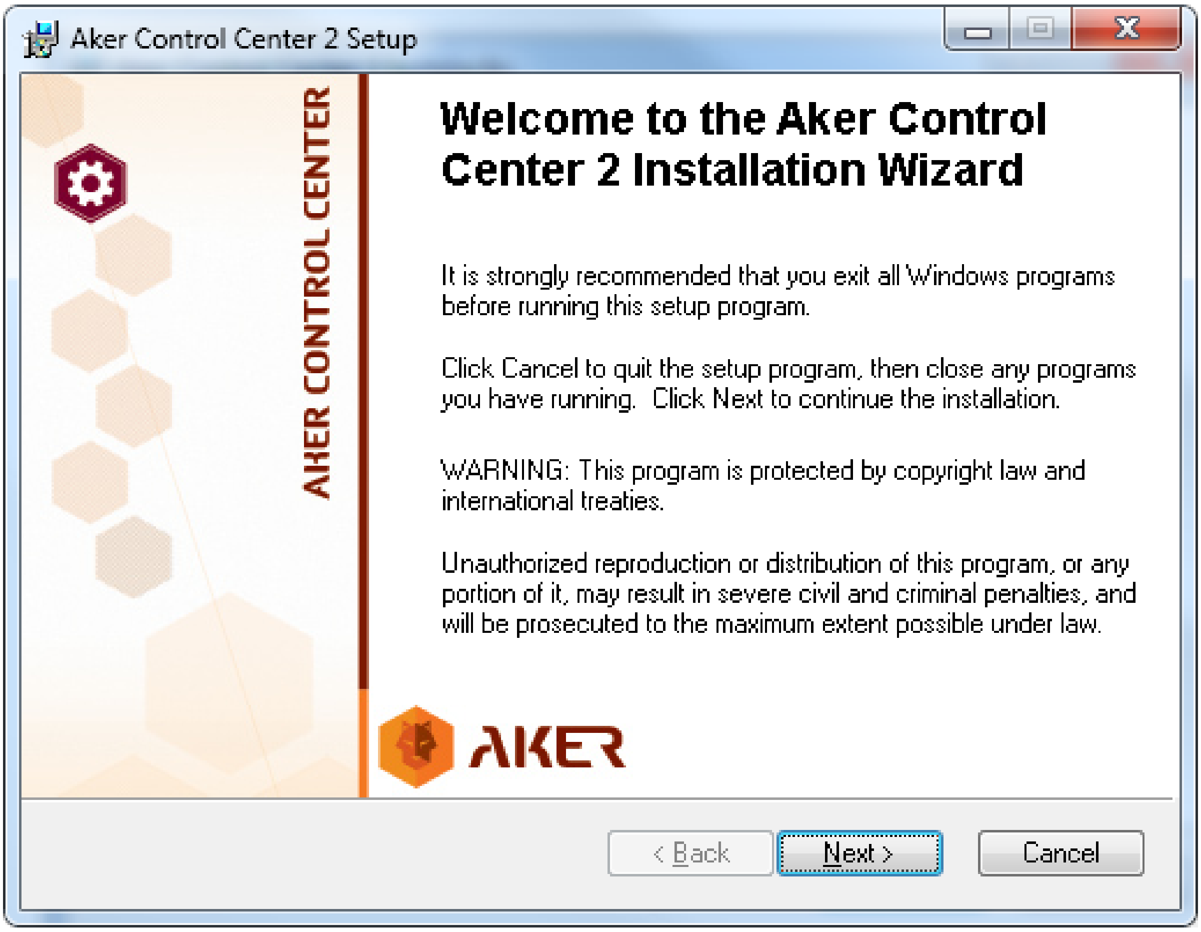
Aker Control Center 2

Please select a language from the list below.

English
Portuguese (Brazil)

Image 1 – Installation language

The following window will be opened: ***'Welcome to Aker control Center 2 Installation Wizard***. Read the recommendations and click on ***"Next"***.



Welcome to the Aker Control Center 2 Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

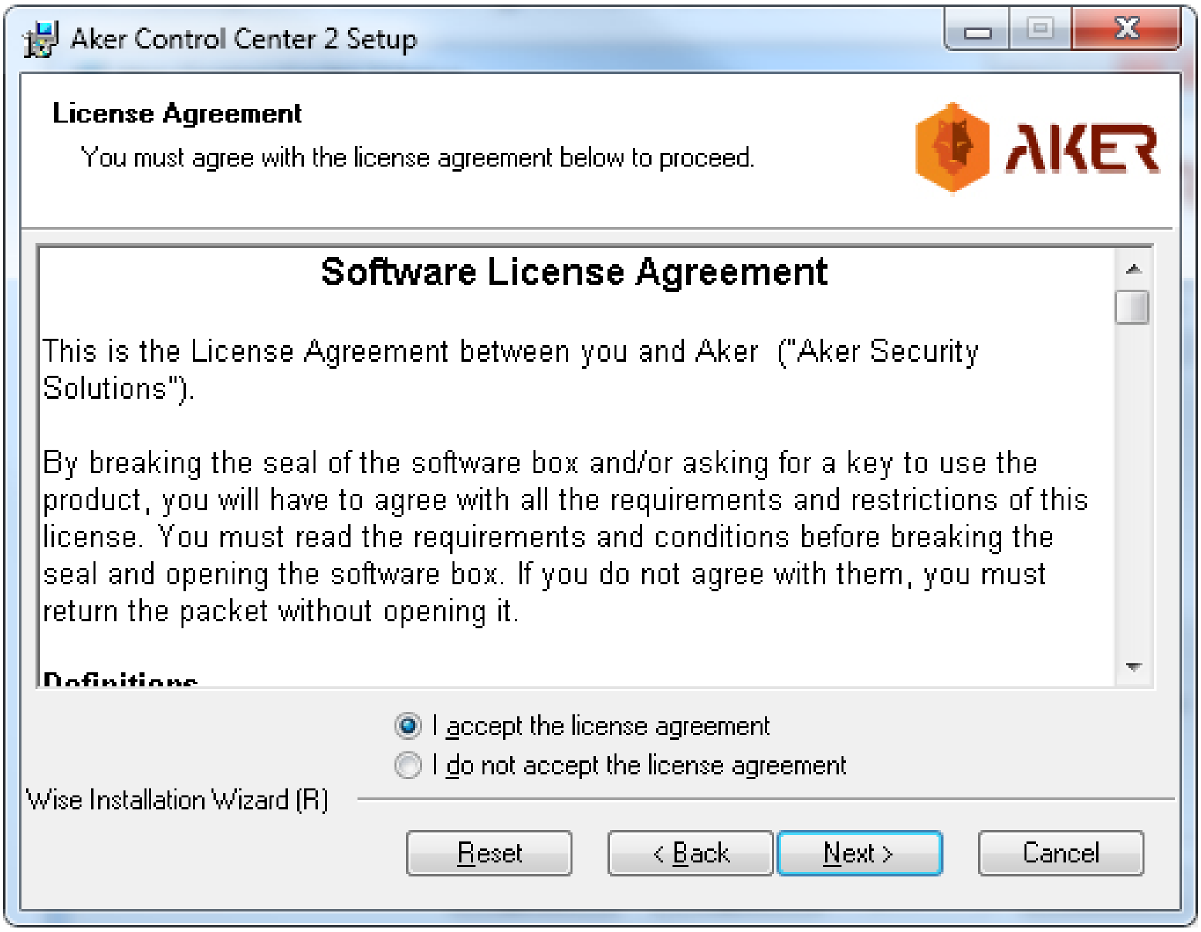
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Image 2 – Aker Control Center 2 Installation (welcome message)

Hereafter, the ***"Program License Agreement"*** window will be displayed. All information should be read.

Select the option "***I accept the License Agreement"*** and click on ***"Next"***.



License Agreement

You must agree with the license agreement below to proceed.

Software License Agreement

This is the License Agreement between you and Aker ("Aker Security Solutions").

By breaking the seal of the software box and/or asking for a key to use the product, you will have to agree with all the requirements and restrictions of this license. You must read the requirements and conditions before breaking the seal and opening the software box. If you do not agree with them, you must return the packet without opening it.

Definitions

● I accept the license agreement

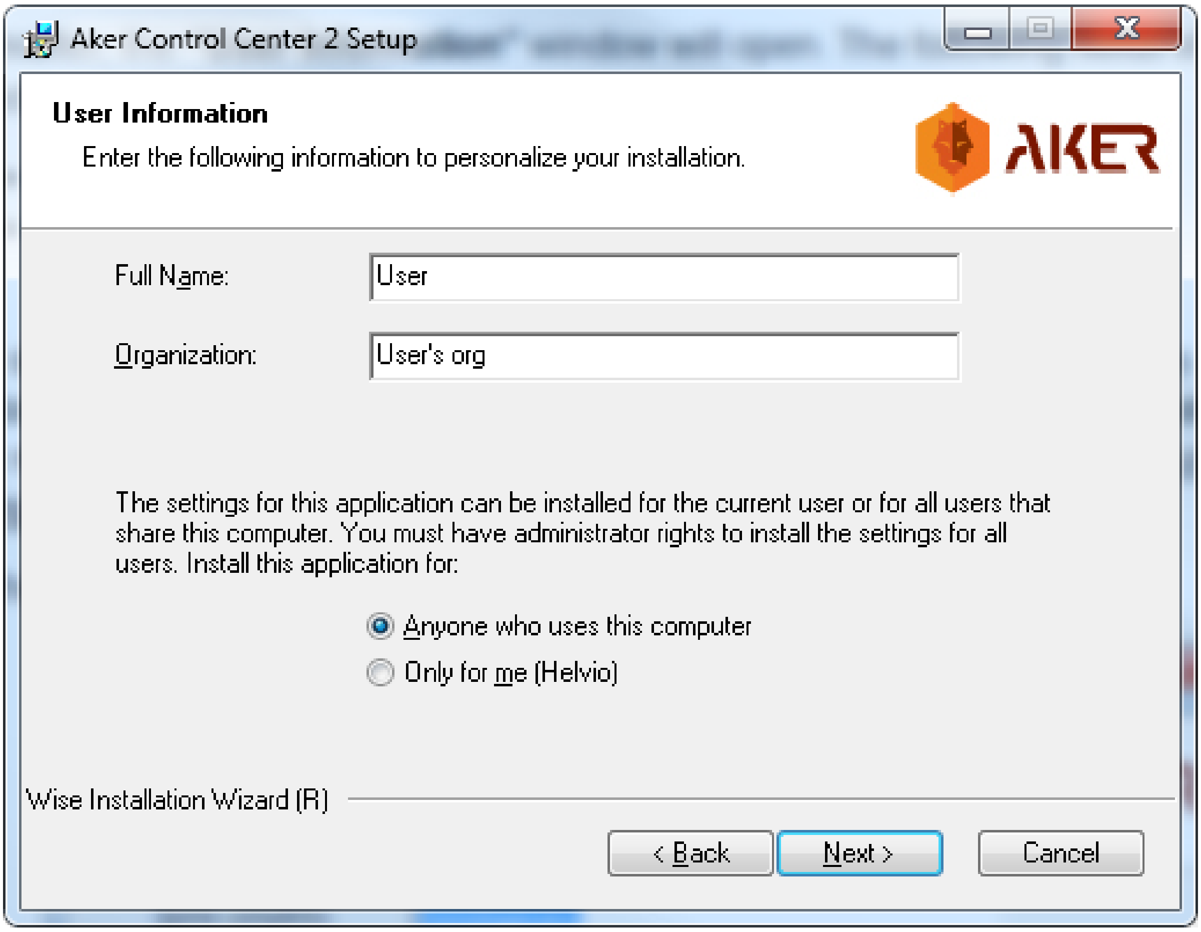
○ I do not accept the license agreement

Image 3 – Software license agreement.

Hereafter, the ***"User Information"*** window will be displayed. The following fields should be filled in:

- **Full name:** user name;
- **Company:** Company name.

As displayed below the text informs that the application configurations may be installed for the current user or all users sharing the computer (administrator rights are required for this). Choose one of the following options: ***'Anyone who uses this computer'*** or ***"Only for me"***, click on ***"Next"***.



User Information

Enter the following information to personalize your installation.

Full Name: User

Organization: User's org

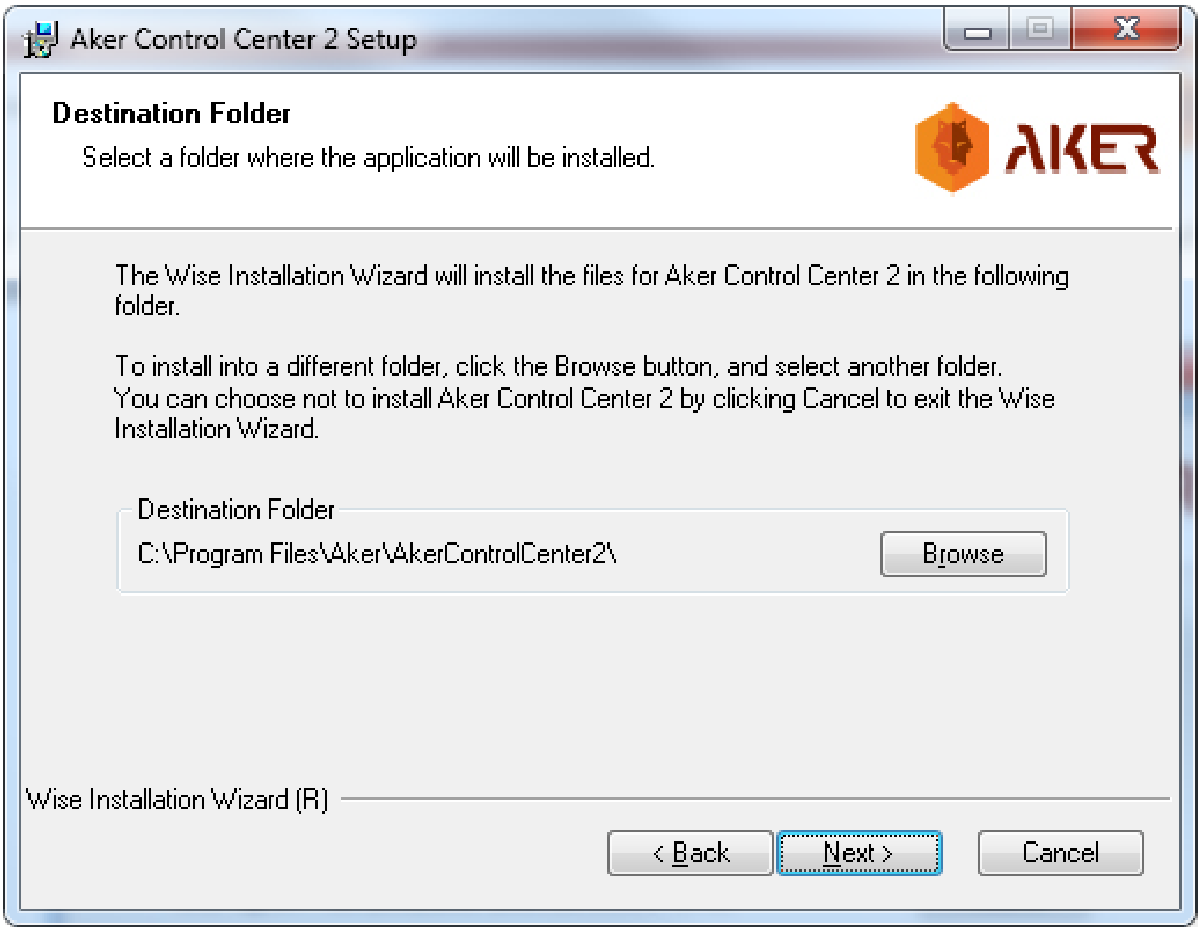
The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:

● Anyone who uses this computer

○ Only for me (Helvio)

Image 4 – User information.

The ***"Destination Folder"*** window allows users to select the folder where the application should be installed.



Aker Control Center 2 Setup

Destination Folder

Select a folder where the application will be installed.

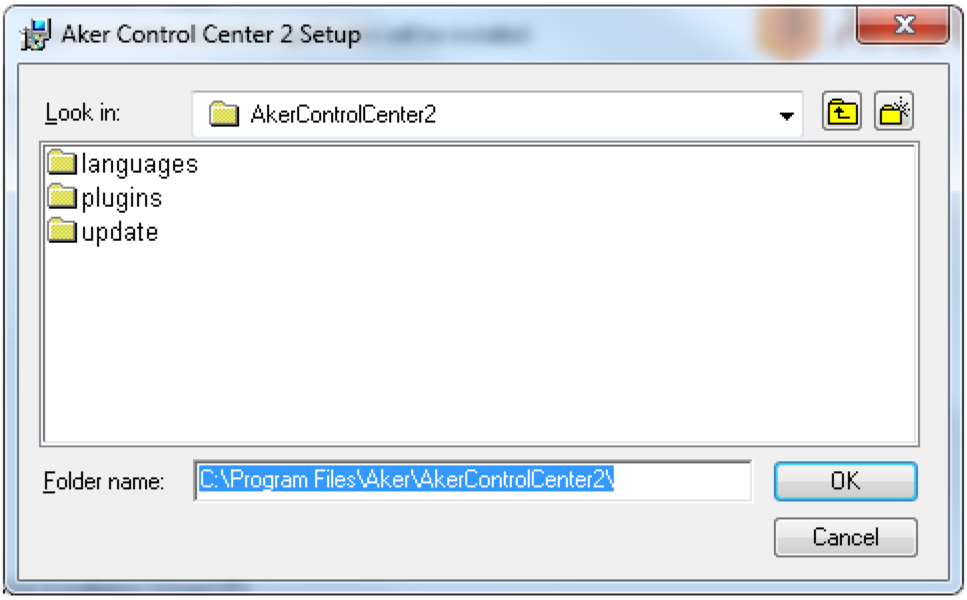
The Wise Installation Wizard will install the files for Aker Control Center 2 in the following folder.

To install into a different folder, click the Browse button, and select another folder.
You can choose not to install Aker Control Center 2 by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder
C:\Program Files\Aker\AkerControlCenter2\

Image 5 – Destination Folder

In case of a specific folder, click on **"Browse"** and the following window will open:



Aker Control Center 2 Setup

Look in: AkerControlCenter2

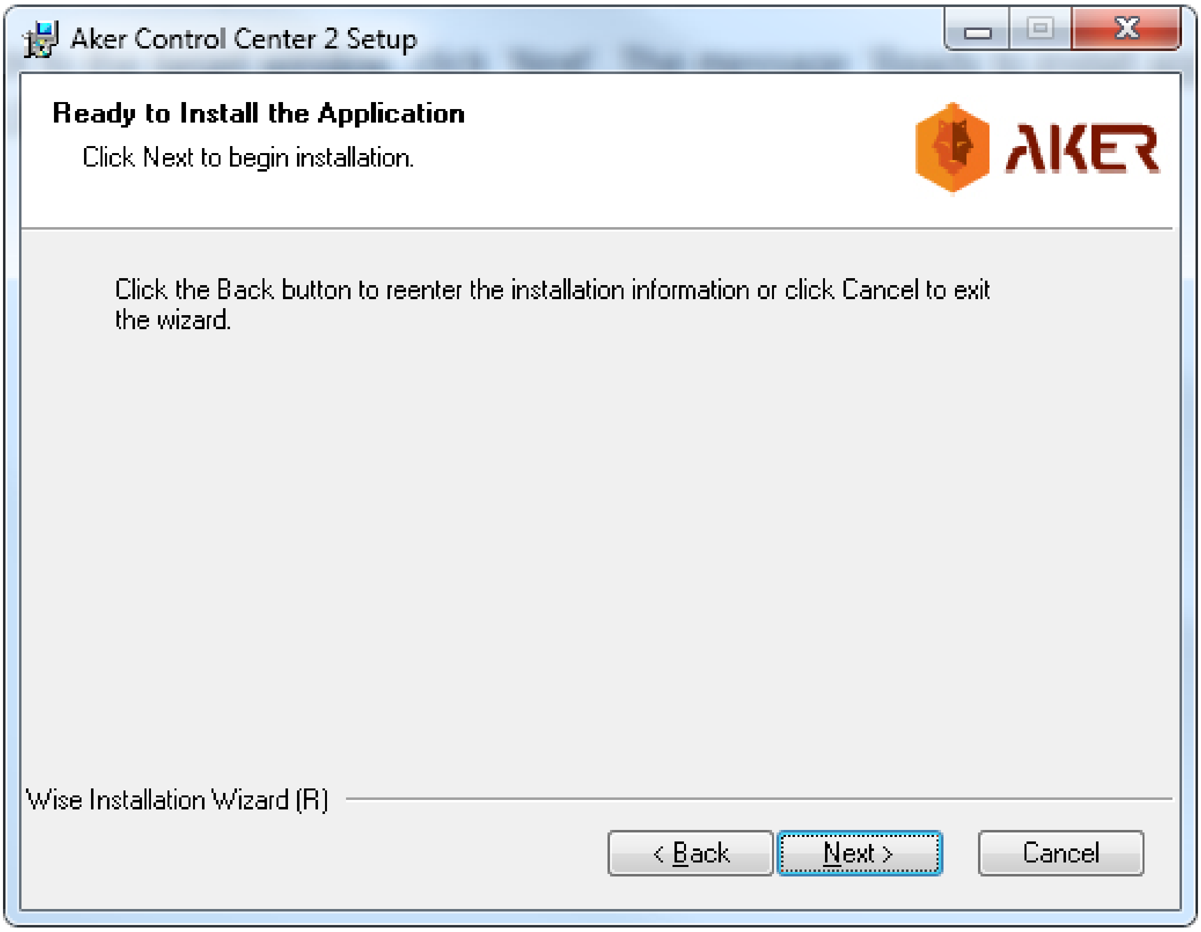
languages
plugins
update

Folder name: C:\Program Files\Aker\AkerControlCenter2\

Image 6 – Installation inside a specific folder.

Search for specific folder and click the ***'OK'*** button.

Back to the Destination window, click on ***"Next"***. The message ***"Ready to install Application"*** will be displayed. Click on ***"Next"*** once again.



Aker Control Center 2 Setup

Ready to Install the Application

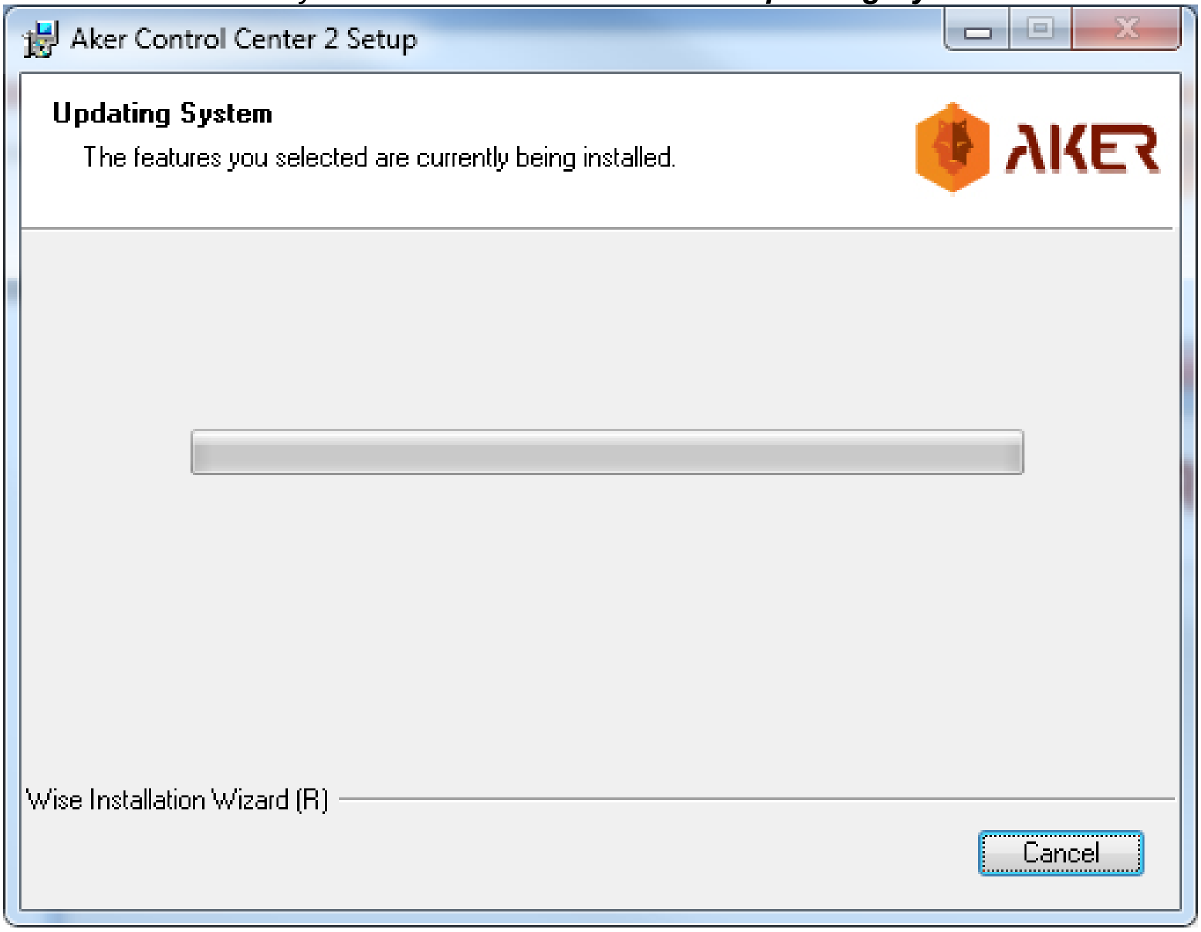
Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

Wise Installation Wizard (R)

Image 7 – Ready to install application

Installation status may be verified on the status bar ***"Updating System"***.



Aker Control Center 2 Setup

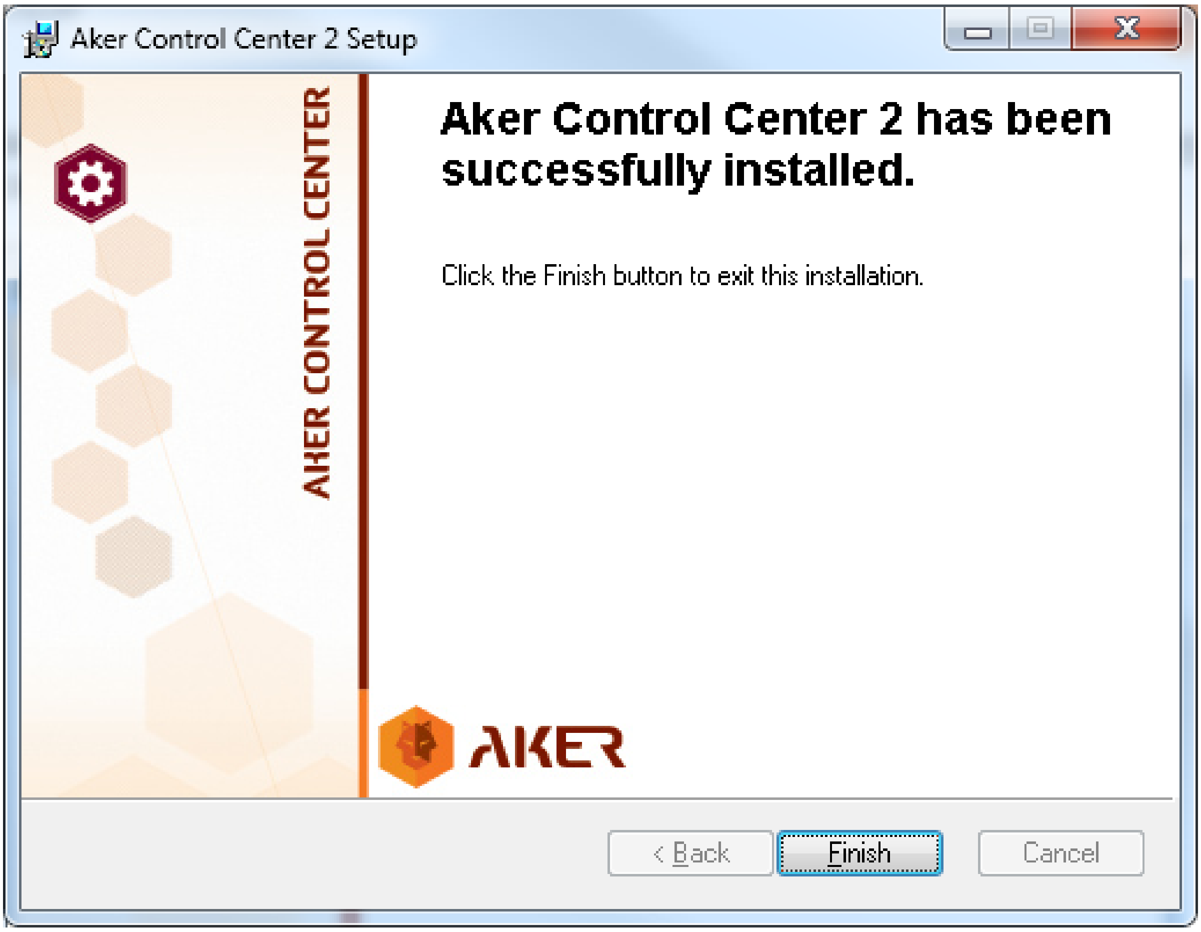
Updating System

The features you selected are currently being installed.

Wise Installation Wizard (R)
Cancel

Image 8 – Installation Bar Status

When installation is complete the message ***"Aker Control Center 2 has been successfully installed"*** will be displayed.



Aker Control Center 2 has been successfully installed.

Click the Finish button to exit this installation.

Image 9 – Successful installation message.

To end installation, just click on ***"Finish"***.

2.3. Aker Firewall Installation

Aker Firewall can be purchased as an appliance, i.e. Firewall Box. When purchased like this, the product is already installed and pre-configured. If you choose to purchase the software (IS version), it should be installed on the chosen computer, this will be explained throughout this topic.

To install it, start your computer with the installation CD-ROM or PEN DRIVE which can be downloaded from Aker website.

To write to the PEN DRIVE, follow the instructions below:

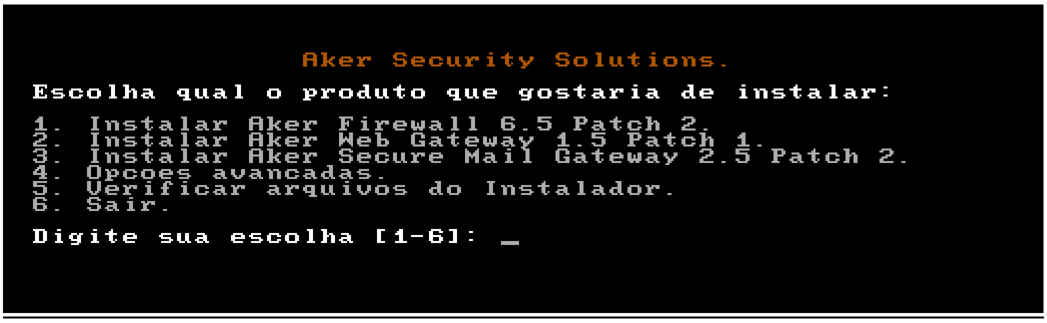
1. Download the file at Aker :www.aker.com.br;
2. Verify if the pen drive on Linux features sdb (type of disk partition), type in the command as root.

“#dmesg | grep sd” or “#fdisk –l” computer disk information will be displayed, find the pen drive.

3. After identifying the device on which Linux has mounted the pen drive, type the following command:
   “dd if=<name of downloaded file> | gunzip | dd of=/dev/<device where the pen drive is>”.
   Example: “dd if=<aker-box-2.0-pt-installer.img.gz | gunzip | dd of=/dev/sdb”
4. All set. Your pen drive is now an Aker products installer.

The following procedure should be performed on the same computer as the Firewall has been installed:

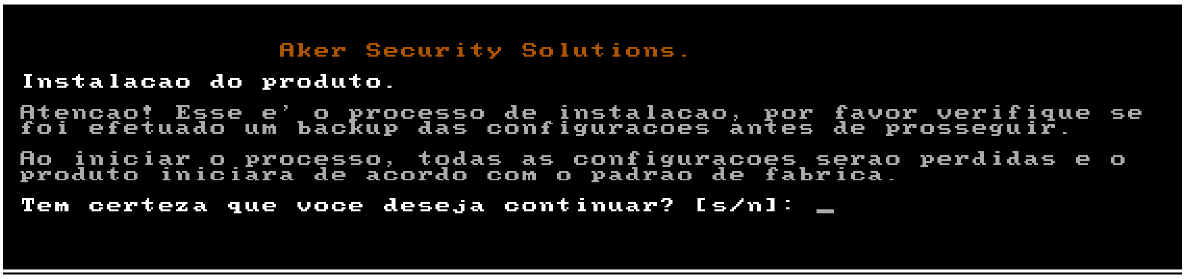
1. Insert the device in the hardware, after this restart the system;
2. Select the product you wish to install: Aker Firewall, Aker Secure Mail Gateway or Aker Web Gateway;



```
                    Aker Security Solutions.
Escolha qual o produto que gostaria de instalar:

1.  Instalar Aker Firewall 6.5 Patch 2.
2.  Instalar Aker Web Gateway 1.5 Patch 1.
3.  Instalar Aker Secure Mail Gateway 2.5 Patch 2.
4.  Opcoes avancadas.
5.  Verificar arquivos do Instalador.
6.  Sair.

Digite sua escolha [1-6]: _
```

Image 10 – Select the product to be installed or configured.

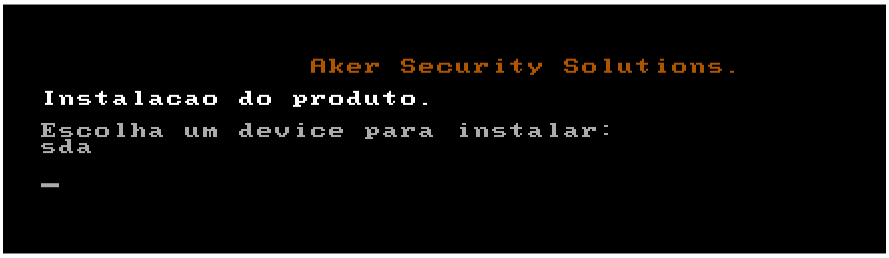
3. Select the **“Install Aker Firewall”** option;
4. Read the following text carefully and confirm installation:



```
                    Aker Security Solutions.
Instalacao do produto.

Atencao! Esse e' o processo de instalacao, por favor verifique se
foi efetuado um backup das configuracoes antes de prosseguir.

Ao iniciar o processo, todas as configuracoes serao perdidas e o
produto iniciara de acordo com o padrao de fabrica.

Tem certeza que voce deseja continuar? [s/n]: _
```

Image 11 – Read the following text carefully and confirm installation.

5. Choose the device which Aker Firewall will be installed on, in this case type in the text “sda”:



```
                 Aker Security Solutions.
 Instalacao do produto.
 Escolha um device para instalar:
 sda

 _
```

Image 12 – Select which disk the product will be installed,

Confirm installation.

6. Installation successfully concluded, click the ***"exit"*** and remove the installation device.

After restarting the computer, the program ***fwinst*** is responsible for performing installation as well as configuring the system for Aker Firewall operation.

2.4. Firewall Aker – Installation Program

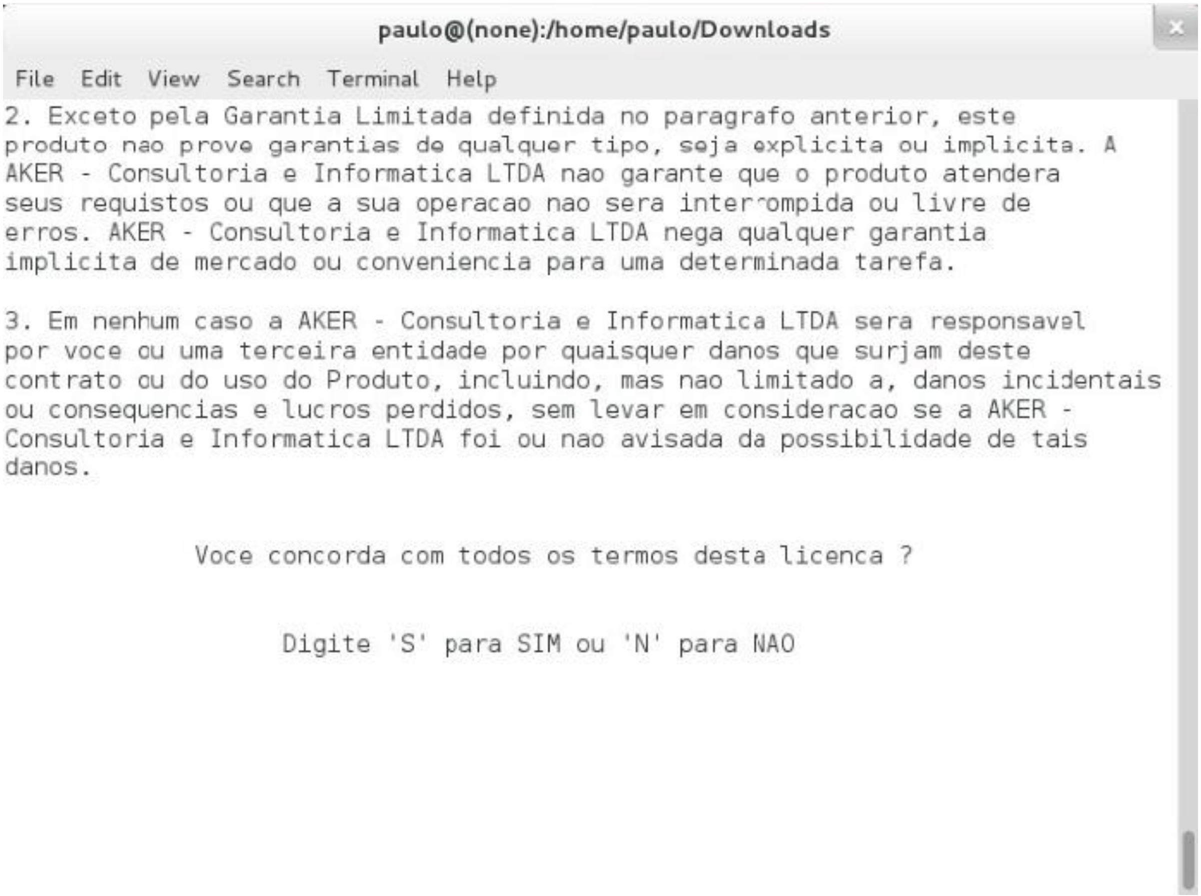
This program performs Aker Firewall Installation as well as text interface and local configurations. The following question will be displayed:

- Do you wish to proceed with the firewall installation (***'Y'*** or ***'N'***)?

After answering **"Yes"**, the installation program will show Aker Firewall usage License. To proceed, it is necessary to accept all terms and conditions within the license. When accepted, the program will continue with the installation process indicating its progress through a series of self-explanatory messages.

After the files have been copied, the installation program will ask questions so the specific system configurations may be executed.

The following window will be displayed:


paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
2. Exceto pela Garantia Limitada definida no paragrafo anterior, este
produto nao prove garantias de qualquer tipo, seja explicita ou implicita. A
AKER - Consultoria e Informatica LTDA nao garante que o produto atendera
seus requistos ou que a sua operacao nao sera interrompida ou livre de
erros. AKER - Consultoria e Informatica LTDA nega qualquer garantia
implicita de mercado ou conveniencia para uma determinada tarefa.

3. Em nenhum caso a AKER - Consultoria e Informatica LTDA sera responsavel
por voce ou uma terceira entidade por quaisquer danos que surjam deste
contrato ou do uso do Produto, incluindo, mas nao limitado a, danos incidentais
ou consequencias e lucros perdidos, sem levar em consideracao se a AKER -
Consultoria e Informatica LTDA foi ou nao avisada da possibilidade de tais
danos.


            Voce concorda com todos os termos desta licenca ?


                  Digite 'S' para SIM ou 'N' para NAO
```

Image 13 – License Term

After answering ‘***Yes***’, all dependencies needed in order to run Aker Firewall will be installed.

System configuration completed. Now it is necessary to activate the installed copy by typing the activation key delivered with the product’s purchase.

The Activation key, company name and external interface IP address should be typed in exactly as they are presented in the document provided by *Aker Consultancy and Informatics* or representatives.

Press ***“Enter”*** to continue.

After this, the program will open a window asking for the pathway where the activation key file has been saved.

In case the activation key is valid the program will proceed with the installation process.

It is necessary to define whether the names of the firewall external network interfaces and IP addresses originating from this interface are not accounted for in the maximum number of the product’s licenses.

External interfaces should take one of the following values:

- eth0;
- eth1;
- eth2.

Insert the external interface: external interface configuration is used for the sole purpose of firewall license control. The name of the interface to be connected to the Internet should be informed.

External interface specifications have no security implications. No access control is made considering this interface.

System activation completed. Now, configure some Aker Firewall parameters. You may now register an IP address to enable the firewall remote administration from another computer. Do you want to register this IP (Y/N)?
After answering **'Yes'**, type the computer IP address where Aker Control Center is installed.

It is possible to automatically register an administrator capable of managing the firewall remotely. This administrator will be granted full rights over the firewall and through him new users can be registered.

In case of NOT registering an administrator, the firewall administration via Remote Interface will not be possible, being local Text Interface the only administration means.

Do you want to create this administrator (Y/N)?

To enable firewall administration via Remote Interface an administrator need to be registered. Either way, it is possible to register an administrator further on via local administration interfaces. The instruction on how to do this, are under the chapter "***Administrating firewall users"***.

If choosing to include a new administrator, a window requesting the data of the new administrator to be registered will open.

2.5. Remote users administration module and including users

Aker Firewall

Enter login: administrator

Enter full name: Aker Firewall Administrator

Enter password (6-14): type in a 6 to 14 letter password.

Confirm password: confirm the password above.

Do you confirm the user inclusion? (Y/N)

After including the user or not, a window will be displayed with a message asking about the registration of a secret shared with Firewall administration via *Aker Configuration Manager*. If you do not have this product, answer ***'No'***, otherwise consult its manual.

Finally a message indicating the installation conclusion and requesting the computer restart for Aker Firewall activation. As soon as the computer is reset the firewall will become automatically operational and may be remotely configured.

Passwords shall have between 6 and 14 letters.

Using Aker Control Center

3. Using Aker Control Center

This chapter deals with the Remote Interface operation of Aker Firewall administration.

3.1. What is Aker Firewall remote administration?

Aker Firewall can be totally configured and administrated from any computer which has a compatible operational system with any remote interface versions, and has TCP/IP which is able to access the computer on which the firewall is installed. This allows a high degree of flexibility and makes administration easier, enabling an administrator to monitor and configure many firewalls from his workstation.

In addition the remote administration saves resources as it allows the host running the firewall does not have monitor or any other peripherals.

The communication between remote interface and Aker products is encrypted with a 256 bits key.

How does Aker Firewall remote administration work*?*

There is a process running on the firewall computer responsible for receiving the connections, this is what makes remote administration possible, it validates users and executes the tasks requested by these users. When a user starts a remote administration session, the Remote Interface establishes a connection with the firewall remote administration module and keeps this connection running all the way until the session is finished by the user.

All communications between remote interface and firewall is performed in a secure way, new encryption keys and authentications are generated at the beginning of each session. Besides this, security techniques are applied to avoid other type of attacks, such as replay attack packets.

Below, there are some comments about important remote administration observations:

In order for the Remote Interface connect to the firewall the addition of a rule is required to release the access *TCP* to port *1020* from the computer which you wish to connect. Information on how to do this can be found on the chapter titled ***Stateful Inspection.***

1. The establishment of a remote administration connection is only possible on a specific moment. If there is an interface already connected, subsequent

connection requests will be denied and the remote interface informs an active session is already in progress.

2. Each remote interface user should be registered in the system. The installation program can automatically create an administrator with rights to register other administrators. In case an administrator is eliminated or has lost his password, it is necessary to use the local Remote Interface or text module to create a new administrator. Details on how to do this can be found on the chapter entitled: ***Administrating Firewall Users***.

3.2. Starting remote interface

To start the Remote Interface, follow the steps bellow:

- For computers running Windows, click the ***'Start'*** menu and select ***'Aker Control Center 2'***.

  The following window will be displayed:

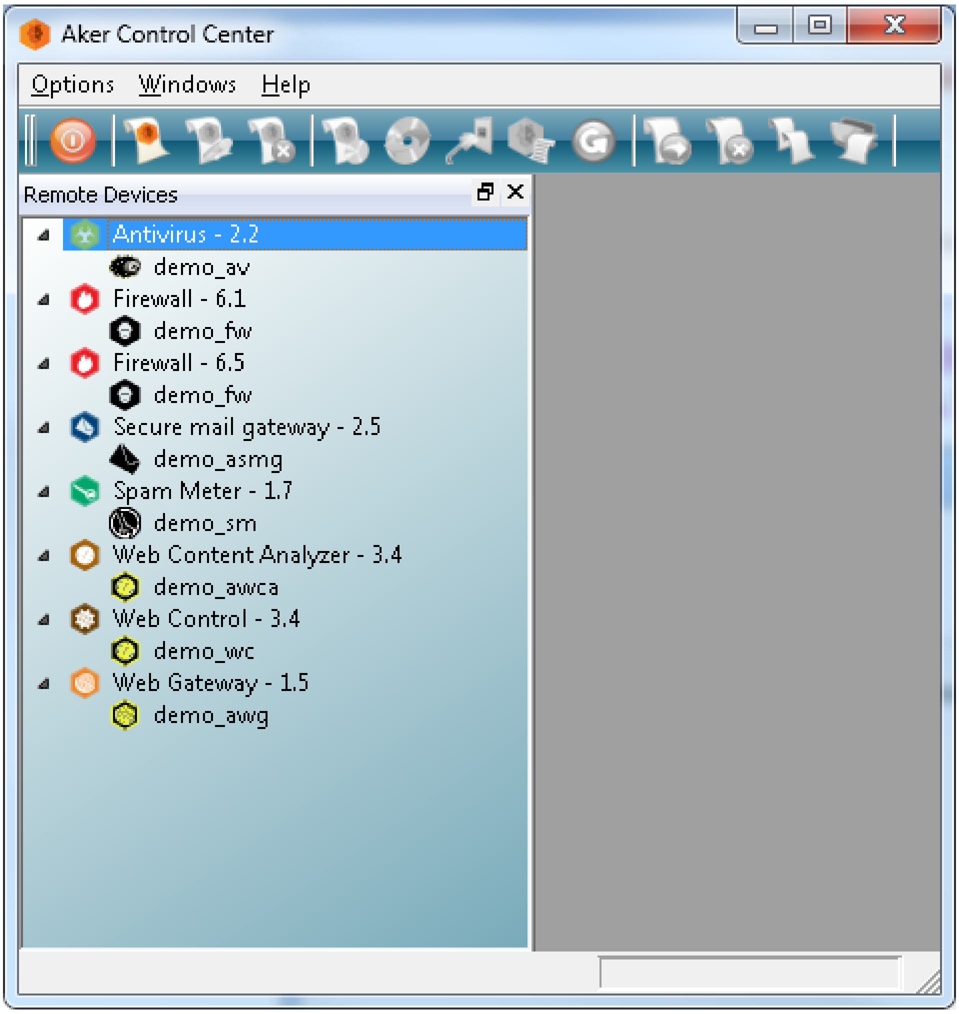

Aker Control Center
Options
Windows
Help
Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
demo_fw
Secure mail gateway - 2.5
demo_asmg
Spam Meter - 1.7
demo_sm
Web Content Analyzer - 3.4
demo_awca
Web Control - 3.4
demo_wc
Web Gateway - 1.5
demo_awg

Image 14 – Accessing Aker Control Center 2

- For computers running Linux, the ***'Control Center'*** installation directory should be accessed and the following *script* executed ***'aker_control_center2_init.sh'.***

The screen above is the main of Aker Firewall and from it; the user can access every configuration option including the Firewall License Activation. Without the ***License Activation*** it is not possible to perform further configurations.

On the first access, all data referring to the license will be in blank and enabled so it can be loaded by the Administrator. The License of Use is located in a file which will be indicated after the ***"Load"*** button is clicked on, as the loaded data is confirmed, a window will open containing all the current license data, then another window will open confirming and restarting the firewall.

Therefore, click on ***"Load"*** at the top right corner of the interface:

The Remote Interface is composed of 4 menus briefly described below (when a firewall is selected a fifth menu is displayed with specific options for itself):

Options

The ***"Options"*** menu contains the settings related to the Remote Interface layout.

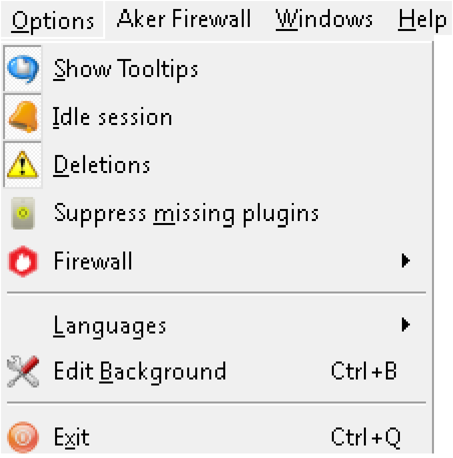
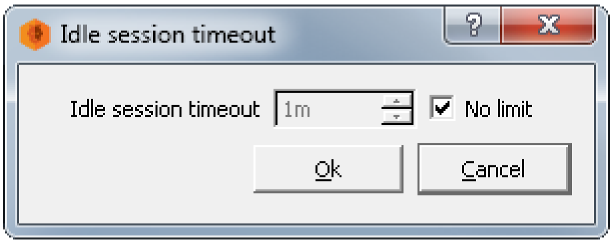


Image 15 – Access window: Options menu.

When clicking this menu, the following options will be displayed:

- **Show Tooltips:** Is the pop up frame which opens when the mouse is passed over an *HTML* element (usually a word in a text) containing additional explanations regarding that element with the mouse arrow over it.
- **Idle session:** Allows a time limit definition, in minutes, of how long the interface will remain connected to the firewall without receiving commands from an administrator. As soon as this time limit is reached, the interface automatically disconnects from the firewall and allows a new connection to be established. These values may vary between 1 e 60 minutes. When the check box entitled ***'Unlimited'*** is checked, the interface will not disconnect from the firewall. Default value of 1 minute. After the changes are made click '***OK***', in case of no changes, click '***Cancel***'.


Idle session timeout
Ok
Cancel

Idle session timeout 1m ☑ No limit

Image 16 – Idle session time.

- **Removal:** In case of removing rules, filters, etc., a message will be sent asking if you really want to remove the selected item;
- **Suppress missing plugins:** In case an Aker plugin has not been installed, this option shows what is missing when clicked on.
- **Firewall:** This menu is used for registering more firewalls in the Remote Interface in a way that it allows the simultaneous administration of many Aker Firewalls to be performed. With the interface connected to two or more firewalls at once it is possible to drag and drop entities and rules between firewalls, making the replication of certain contents between them easier. Within the Firewall menu, we have:

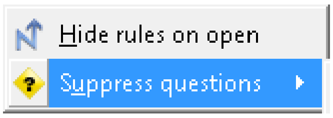

Hide rules on open
Suppress questions

Image 17 – Hide rules.

- **Hide rules: collapses rule policies.**

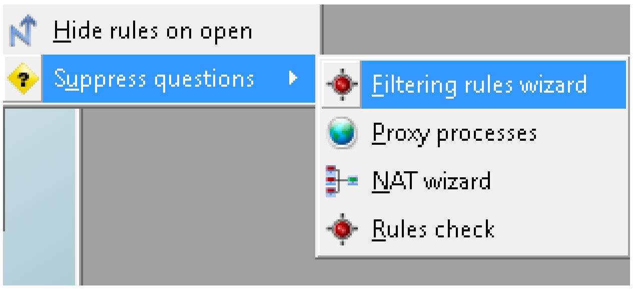

Hide rules on open
Suppress questions
Filtering rules wizard
Proxy processes
NAT wizard
Rules check

Image 18 – Disable questions.

  - **Disable questions**

    - **Filtering rules wizard:** filtering rule creation assistant;
    - **Nat wizard:** creates Nat rules;
    - **Rule Check:** Filtering rules checker scanning for overlapping rules.

- **Languages:** Switches between both languages which the Remote Interface can be accessed in (English or Portuguese).

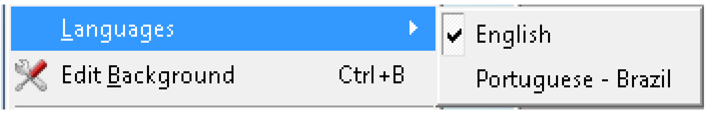

Languages
Edit Background Ctrl+B
English
Portuguese - Brazil

Image 19 – Choose the language you wish to access Aker Control Center.

- **Edit background:** it is possible to choose and redefine the background color which you wish to work. Further explanation about this shall be given later on;

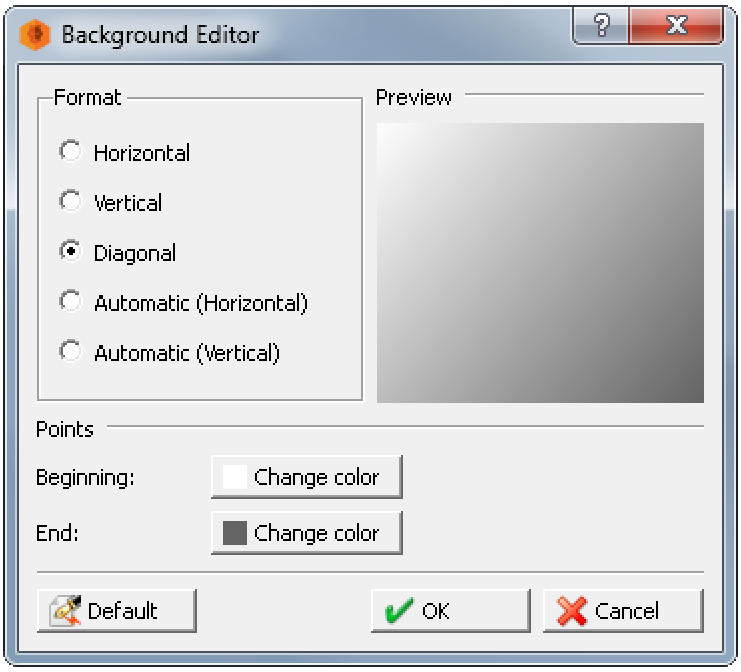

Background Editor
Format
Horizontal
Vertical
Diagonal
Automatic (Horizontal)
Automatic (Vertical)
Preview
Points
Beginning:
Change color
End:
Change color
Default
OK
Cancel

Image 20 – Aker Control Center background color

  - **Format:** defines the Aker Control Center screen format :

Image 21 – Horizontal format.

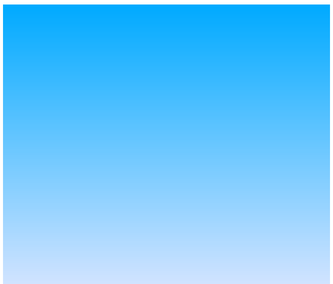


Image 22 – Vertical format.

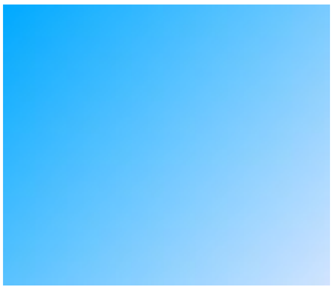


Image 23 – Diagonal format.

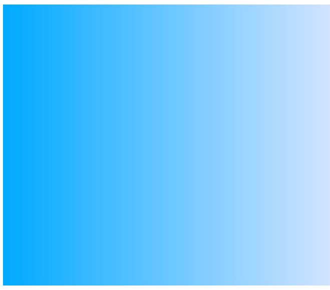


Image 24 – Automatic horizontal.

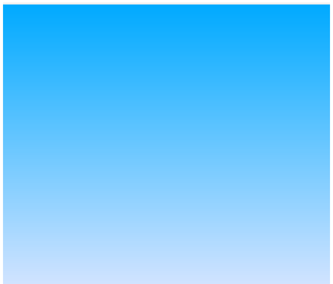
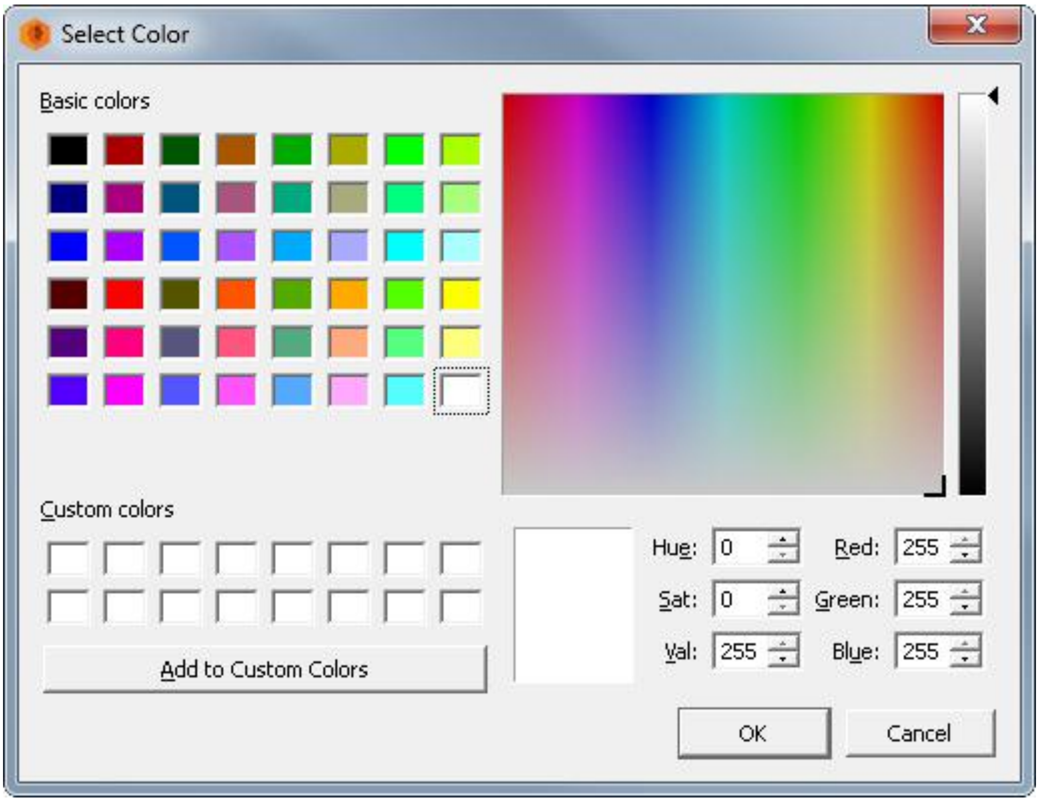


Image 25 – Automatic vertical format.

- **Dots:** initial and final colors can be changed, just select the color and click ***‘OK’***.


Select Color
Basic colors
Custom colors
Add to Custom Colors
OK
Cancel

Hue: 0
Sat: 0
Val: 255
Red: 255
Green: 255
Blue: 255

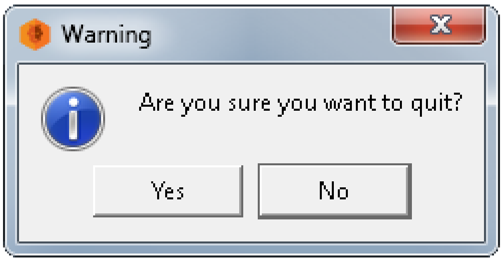
Image 26 – Select color.

- ○ **Default Option:** when this option is selected the screen will proceed with an Aker default configuration.

Image 27 – Button: Default.

After making your choice, click ***'OK'***.

- **Exit:** when the exit option is selected, the screen below will appear asking for confirmation:


Warning
Yes
No

Are you sure you want to quit?

Image 28 – Exit warning.

To close the interface program click ***'Yes'*** or to keep it running click ***'No'***.

Windows Menu

The *Windows menu* contains the configuration functions of all the opened windows, and also the menu bar.

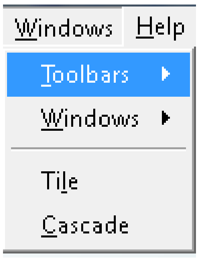

Windows
Help
Toolbars
Windows
Tile
Cascade

Image 29 – Windows menu.

- **Toolbars:** this option allows you to decide whether the Toolbars will be displayed at top or not.
- **Windows:** shows remote device items (this option may also be accessed by hitting the ***'F9'*** key on the keyboard)**.**

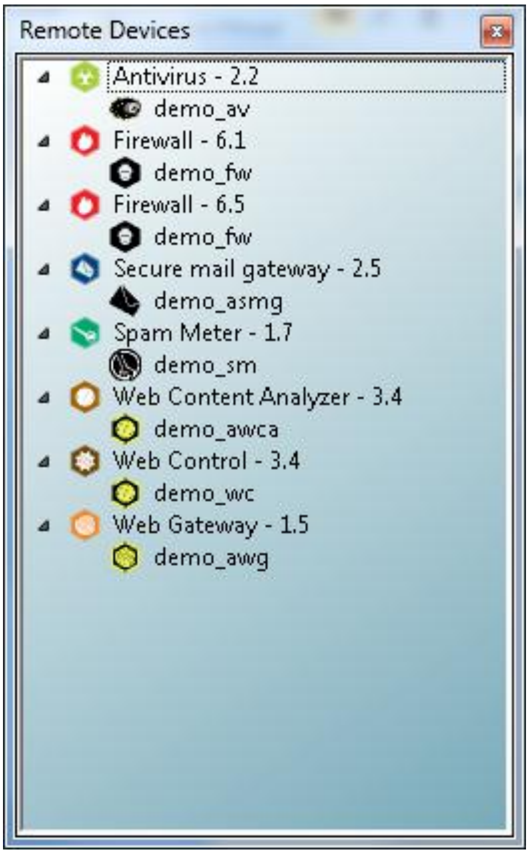
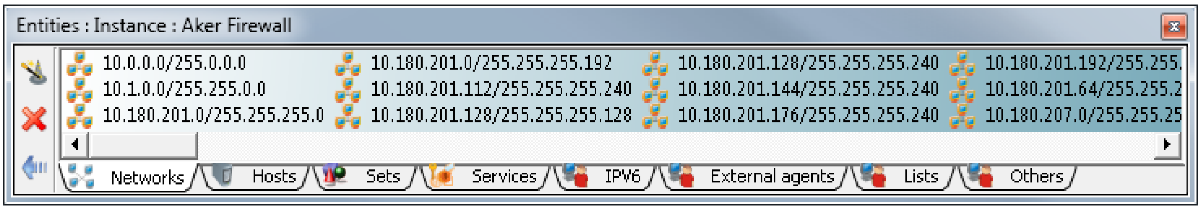

Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
demo_fw
Secure mail gateway - 2.5
demo_asmg
Spam Meter - 1.7
demo_sm
Web Content Analyzer - 3.4
demo_awca
Web Control - 3.4
demo_wc
Web Gateway - 1.5
demo_awg

Image 30 – Access Window: remote devices.

- **Entities:** shows the entities (may be accessed by hitting the ***'F9'*** key on the keyboard).


Entities : Instance : Aker Firewall
Networks
Hosts
Sets
Services
IPV6
External agents
Lists
Others

10.0.0.0/255.0.0.0
10.1.0.0/255.255.0.0
10.180.201.0/255.255.255.0
10.180.201.0/255.255.255.192
10.180.201.112/255.255.255.240
10.180.201.128/255.255.255.128
10.180.201.128/255.255.255.240
10.180.201.144/255.255.255.240
10.180.201.176/255.255.255.240
10.180.201.192/255.255.
10.180.201.64/255.255.2
10.180.207.0/255.255.25

Image 31-Access Window: entities.

- **Tile:** when this option is selected, the open windows on the right side of the Remote Interface will be adjusted in a way all of them will be simultaneously visible.
- **Cascade:** this option organizes the open windows on the right side of the Remote Interface placing one in front of the other, in cascade.

Windows:

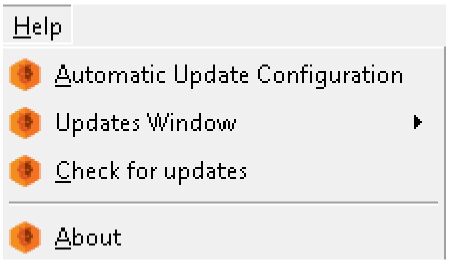
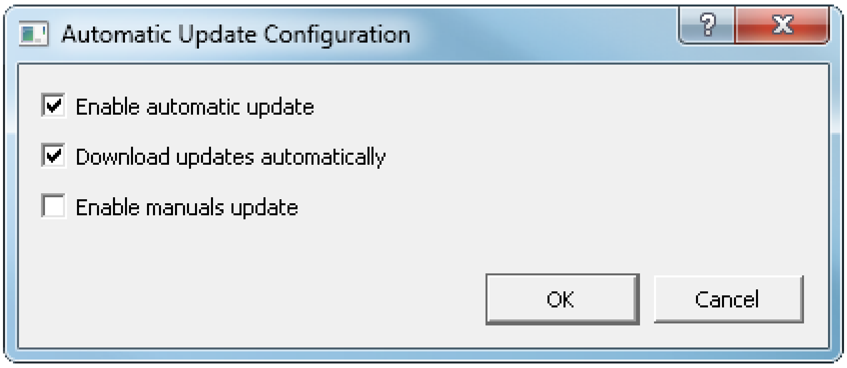

Help
Automatic Update Configuration
Updates Window
Check for updates
About

Image 32-Access Window: windows.

- **Automatic update configuration:** allows automatic configuration. Through this window it is possible to ***"Enable automatic update"***, ***"Download updates automatically"***, and also ***"Enable manuals update"***.


Automatic Update Configuration
OK
Cancel

☑ Enable automatic update
☑ Download updates automatically
☐ Enable manuals update

Image 33 – Automatic Update Configuration

Once the options have been selected, just **click on "OK".**

- **Update Windows**: this menu contains the Download Windows items where the necessary updates are presented for download.

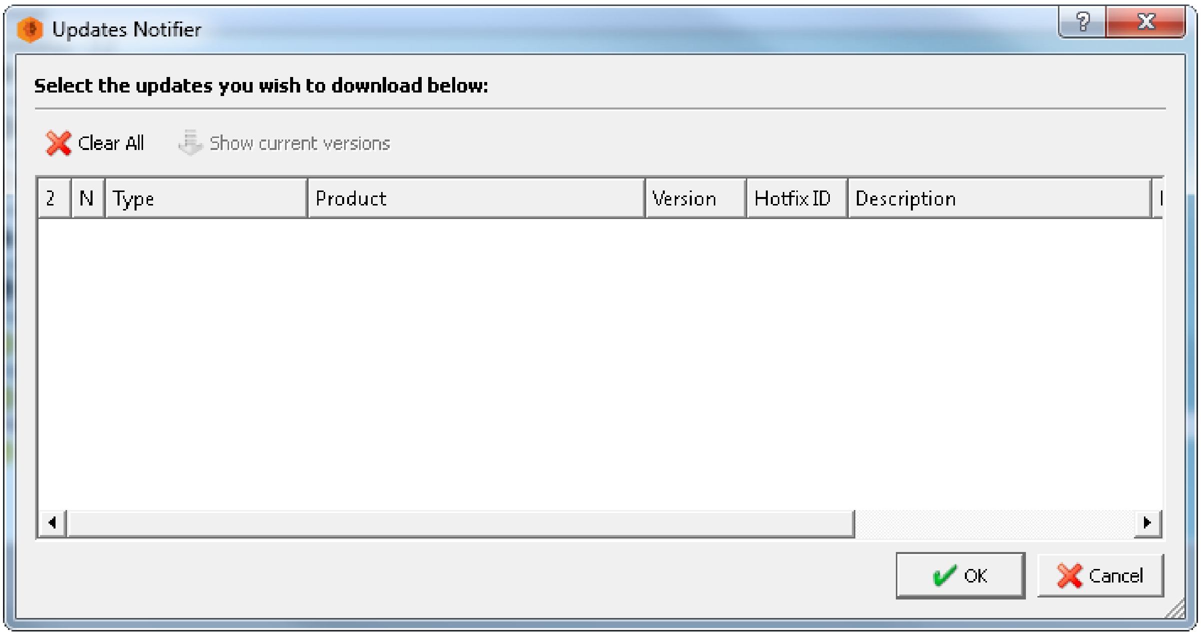

Updates Notifier
Select the updates you wish to download below:
Clear All
Show current versions
2
N
Type
Product
Version
Hotfix ID
Description
OK
Cancel

Image 34 – Update Notifier

The ***"Update Installation Notifier"*** allows the selection of updates to be installed.

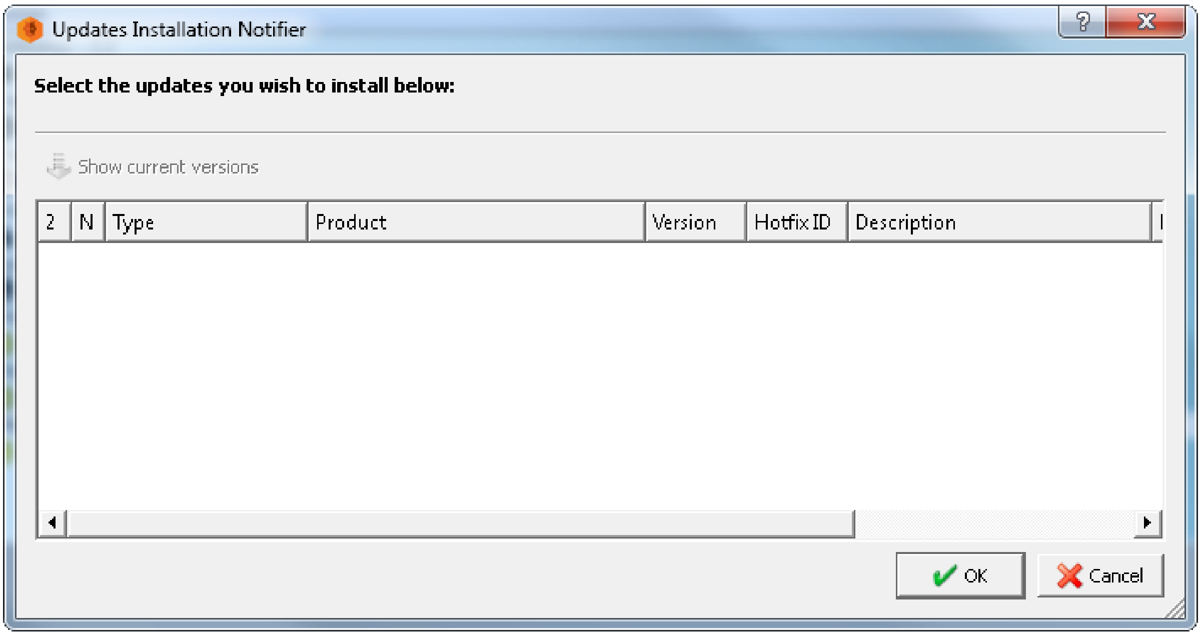
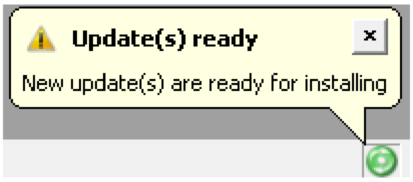

Updates Installation Notifier
Select the updates you wish to install below:
Show current versions
2
N
Type
Product
Version
Hotfix ID
Description
OK
Cancel

Image 35-Update Installation Notifier

- **Update Search:** by selecting this option, a search for pending updates is performed, as indicated by the Image below:

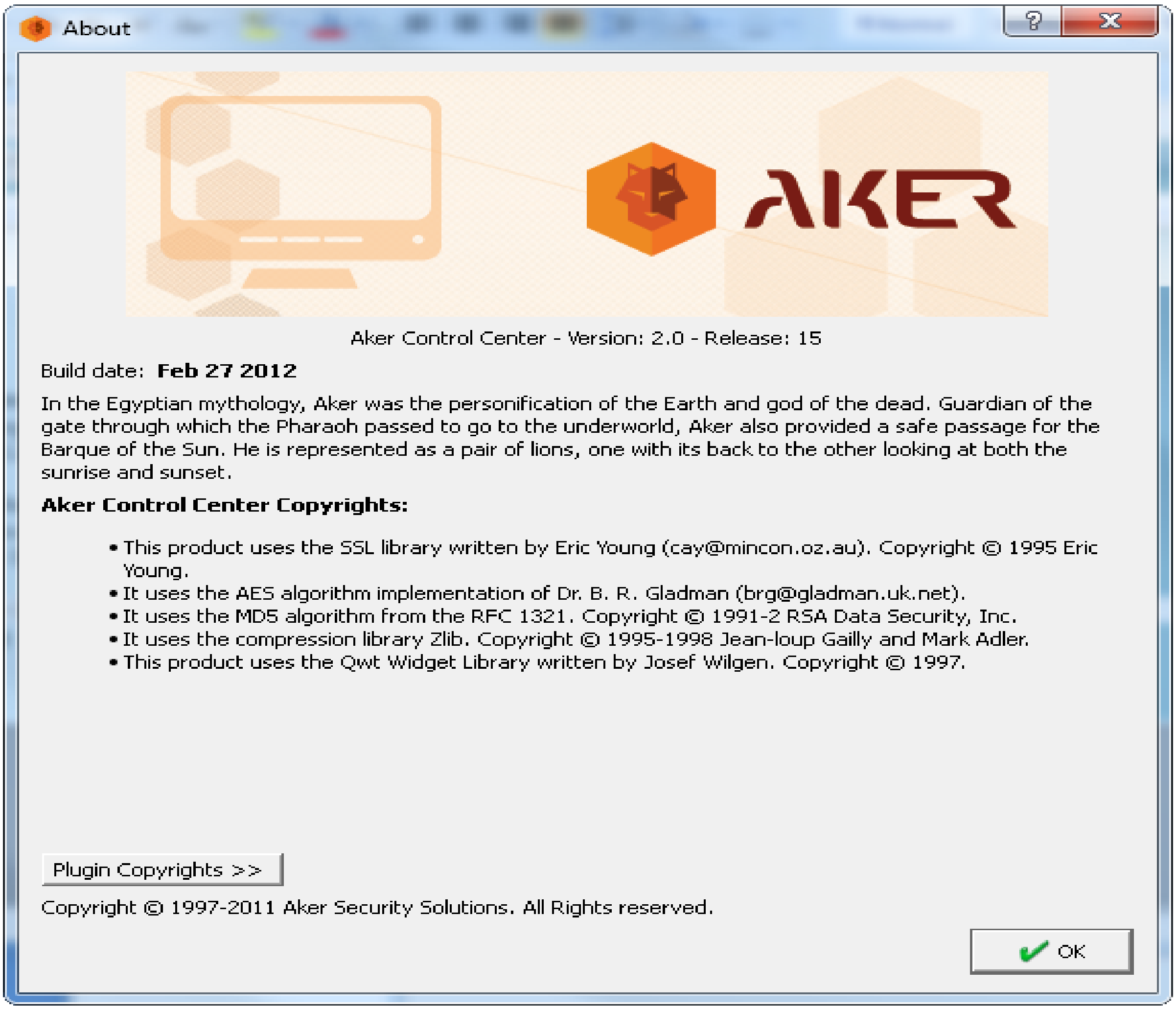


Update(s) ready

New update(s) are ready for installing

Image 36 – Updates(s) ready.

- **About:** shows information about Aker Control Center.



Aker Control Center - Version: 2.0 - Release: 15

Build date: **Feb 27 2012**

In the Egyptian mythology, Aker was the personification of the Earth and god of the dead. Guardian of the gate through which the Pharaoh passed to go to the underworld, Aker also provided a safe passage for the Barque of the Sun. He is represented as a pair of lions, one with its back to the other looking at both the sunrise and sunset.

Aker Control Center Copyrights:

- This product uses the SSL library written by Eric Young (cay@mincon.oz.au). Copyright © 1995 Eric Young.
- It uses the AES algorithm implementation of Dr. B. R. Gladman (brg@gladman.uk.net).
- It uses the MD5 algorithm from the RFC 1321. Copyright © 1991-2 RSA Data Security, Inc.
- It uses the compression library Zlib. Copyright © 1995-1998 Jean-loup Gailly and Mark Adler.
- This product uses the Qwt Widget Library written by Josef Wilgen. Copyright © 1997.

Copyright © 1997-2011 Aker Security Solutions. All Rights reserved.

Image – 37 Information on the topic (About)

To close, click on ***'OK'***.

Aker Firewall

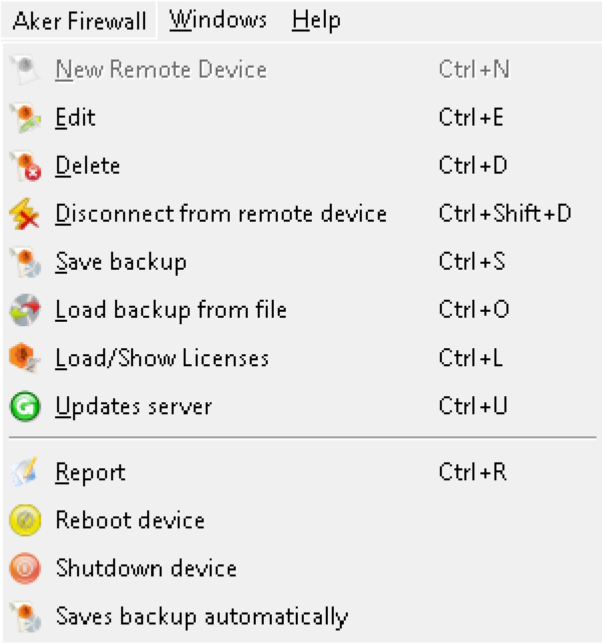

Aker Firewall
Windows
Help
New Remote Device Ctrl+N
Edit Ctrl+E
Delete Ctrl+D
Disconnect from remote device Ctrl+Shift+D
Save backup Ctrl+S
Load backup from file Ctrl+O
Load/Show Licenses Ctrl+L
Updates server Ctrl+U
Report Ctrl+R
Reboot device
Shutdown device
Saves backup automatically

Image 38-Access Window: Aker Firewall.

Not every option on the menus will be enabled due to the fact they only work when there is a connection established. To gain access to the others options, a remote administration session should be established with the firewall you wish to administrate. Therefore, the following steps should be followed:

Register the firewall selecting the ***‘Firewalls’*** menu and the ***‘New Firewall’*** option (check the item ***“Registering Firewall”***);

Select the desired firewall for connection

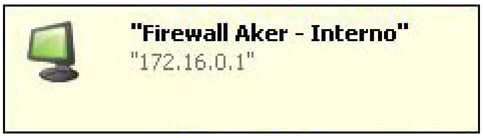
Click on the Connect option.

- **New Remote Device:** Registers a new device
- **Edit:** performs editions;
- **Delete**: deletes devices;
- **Connect to selected device**: connects to device;
- **Reboot device:** restarts device;
- **Shutdown device**: turns the remote device off;
- **Save backup automatically:** backups are saved.

Items described above will be addressed in the next pages.

- **Text on buttons:** by marking this option each corresponding action button icon will be displayed. By unchecking this option, only the icon will be displayed.

- **Hints for Entities:** when this option is activated, a small box containing the description of each entity will be displayed when the mouse is passed over the respective icons.



"Firewall Aker - Interno"
"172.16.0.1"

Image 39 – Entity description box.

- **Show icons on buttons:** this option, when activated, enables icons to be displayed on the ***"OK"***, ***"Cancel"*** and ***"Apply"*** window buttons.

Windows: this option allows showing or not, the default window of the system: ***"help"***, ***"firewalls"*** and ***"entities"***.

Firewalls registration

In this section we will deal with how to register one or more firewalls when the ***"New remote device"*** option is selected from within the ***"Firewalls"*** menu or through the icon "***Create remote device"*** icon.

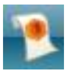
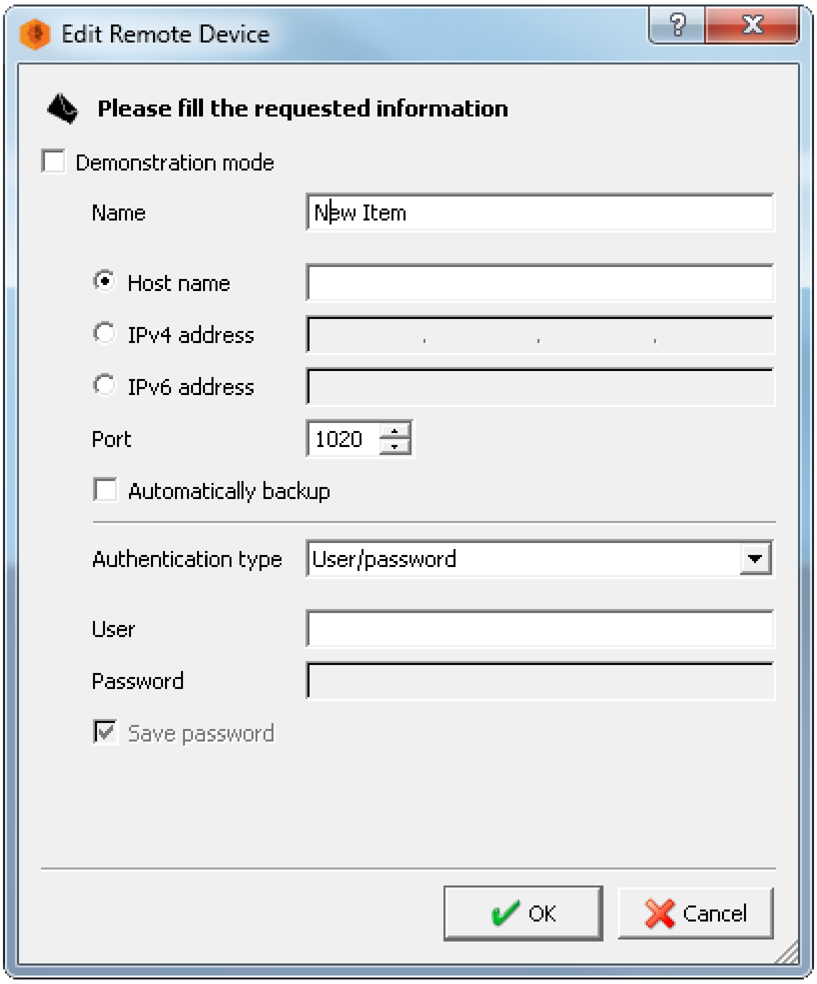


Image 40 – Button**:** Create a new remote device.

The ***“Edit Remote Device”*** window will pop up and the desired kind of authentication may be chosen. According to each option the window will be changed, showing the corresponding fields.

Authentication type: User/Password



Edit Remote Device

Please fill the requested information

☐ Demonstration mode

Name: New Item

● Host name

○ IPv4 address

○ IPv6 address

Port: 1020

☐ Automatically backup

Authentication type: User/password

User

Password

☑ Save password

Image 41 – Remote device authentication box.

Demonstration mode: When this mode is selected, a demo firewall with default configuration will be created. No real connection will be established under any attempt to connect it, any number of demo firewalls may be created, each one with distinct configurations from another.

Name: registers the name under which the firewall will be referred to, in the Remote Interface;

Host name: In case the firewall server which you wish to connect has a name associated to the computer IP address, simply place this name in this option so the Control Center can automatically resolve the *DNS* and connect itself into the server;

IPv4 and IPv6 Addresses: registers IP address to connect to the firewall.

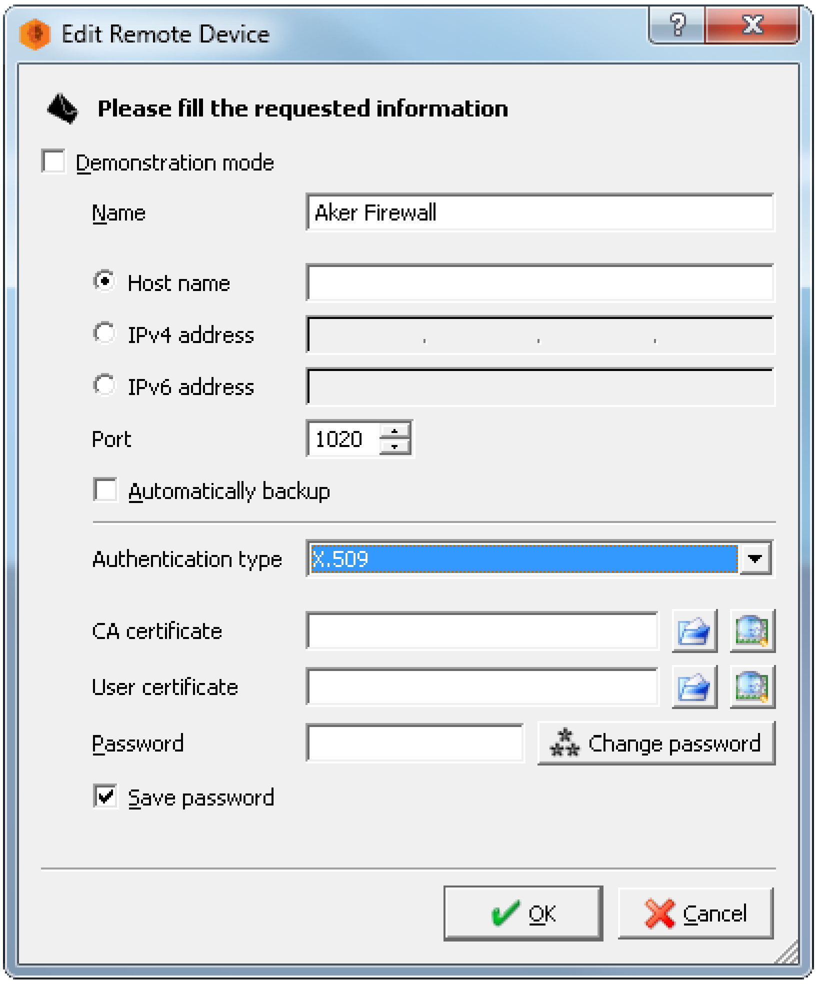
User: this field identifies the user accessing the firewall. It records and keeps a track of users each time the firewall is accessed.

Password: the user password. In case the ***"Save Password"*** box is checked, will not be necessary type the password when the connection is performed (password will show on the screen as many asterisks **"*"**). If this box is unchecked, means the field will be disabled.

Every 3 invalid attempts the client is blocked from accessing the Control Center for 3 minutes. Each invalid attempt generates an "Excessive invalid attempts" event of the Firewall Daemons module.

At the end, just click ***'OK'*** and the firewall will be registered, with the selected authentication type. In case of cancelling registration, just click ***'Cancel'***.

Authentication Type: X.509



☐ Demonstration mode

Name: Aker Firewall

● Host name

○ IPv4 address

○ IPv6 address

Port: 1020

☐ Automatically backup

Authentication type: X.509

CA certificate

User certificate

Password

☑ Save password

Image 42 – Required information to Edit Remote Device.

This option allows authentication with X.509 digital certification.

CA Certificate: represents the root certificate of the certificate authority, and show the certificate Domain common name (C.N).

By clicking on the icon displayed below, a '*.cer/*.crt' extension file containing the certificate will be loaded.

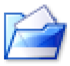


Image 43 – Icon used to load files.

The following icon shows a summary of certificate information.

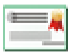


Image 44 – Icon used to show certificate information.

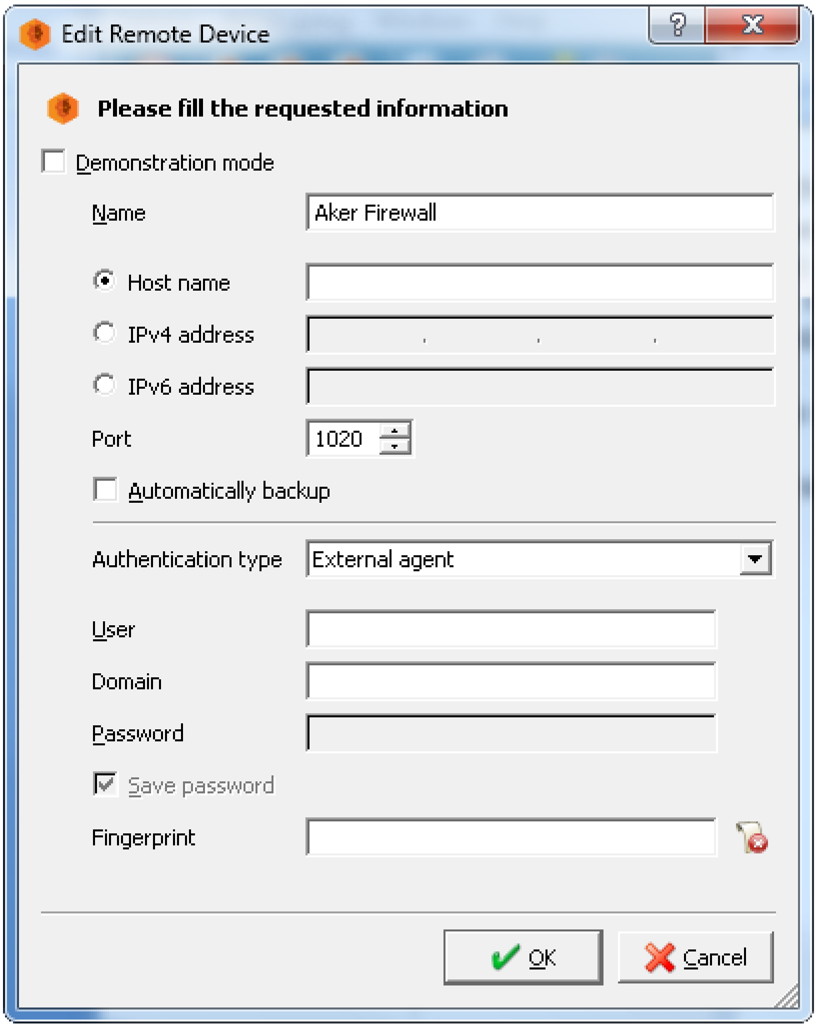
User Certificate: this option allows a packet in ***PKCS#12*** format. The packet is dismembered into two files, one containing the certificate itself and the other containing the key. The certificate is loaded with one password and the other is to save the key file, saving it as encrypted.

Password: The password under which the primary key has been saved. If informed (registry) it unscramble the key and sends it to the firewall perform an authentication. In case the ***'Save Password'*** box remains marked, it will not be necessary to type passwords when a connection is established (the password will be displayed in the screen as many asterisks '*'). In case it is unmarked, this field will be disabled.

Change Password: Changes the password registered on the password field.

Save Password: Allows the password to be automatically saved.

Authentication Type: External agent user/password



☐ Demonstration mode

Name: Aker Firewall

● Host name

○ IPv4 address

○ IPv6 address

Port: 1020

☐ Automatically backup

Authentication type: External agent

User

Domain

Password

☑ Save password

Fingerprint

Image 45 – Authentication types (user, domain and password) to edit Remote Device.

This option allows authentication through ***External Agents***.

User: The user who access the firewall. This field records user and where the user will be displayed every time the firewall is accessed.

Domain: Domain name on which the external agent is running.

Password: User password. In case the ***"Save Password"*** box remains checked, typing in the password when connecting is no longer necessary (the password will appear on screen as many asterisks **'*'**). In case it is unchecked, this field will remain disabled.

Fingerprint: This is a summary of the firewall digital certificate identification. This option enables the user to identify when there has been a change to the firewall to which connection is desired.

Observation: During the first connection attempt there will be no firewall identification. From the second time onwards, every time it is connected it will compare with the fingerprint.

Eraser Fingerprint: Reset and begin from initial stage. If there is a change on the firewall, the identification will be different, then the connection will not be possible, only if erase fingerprint is clicked on.

After the firewall is registered, the recently created firewall icon, on the left side of the window, can be double-clicked, or clicked on once to select it, and then click on the ***'Connect'*** button.

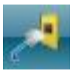
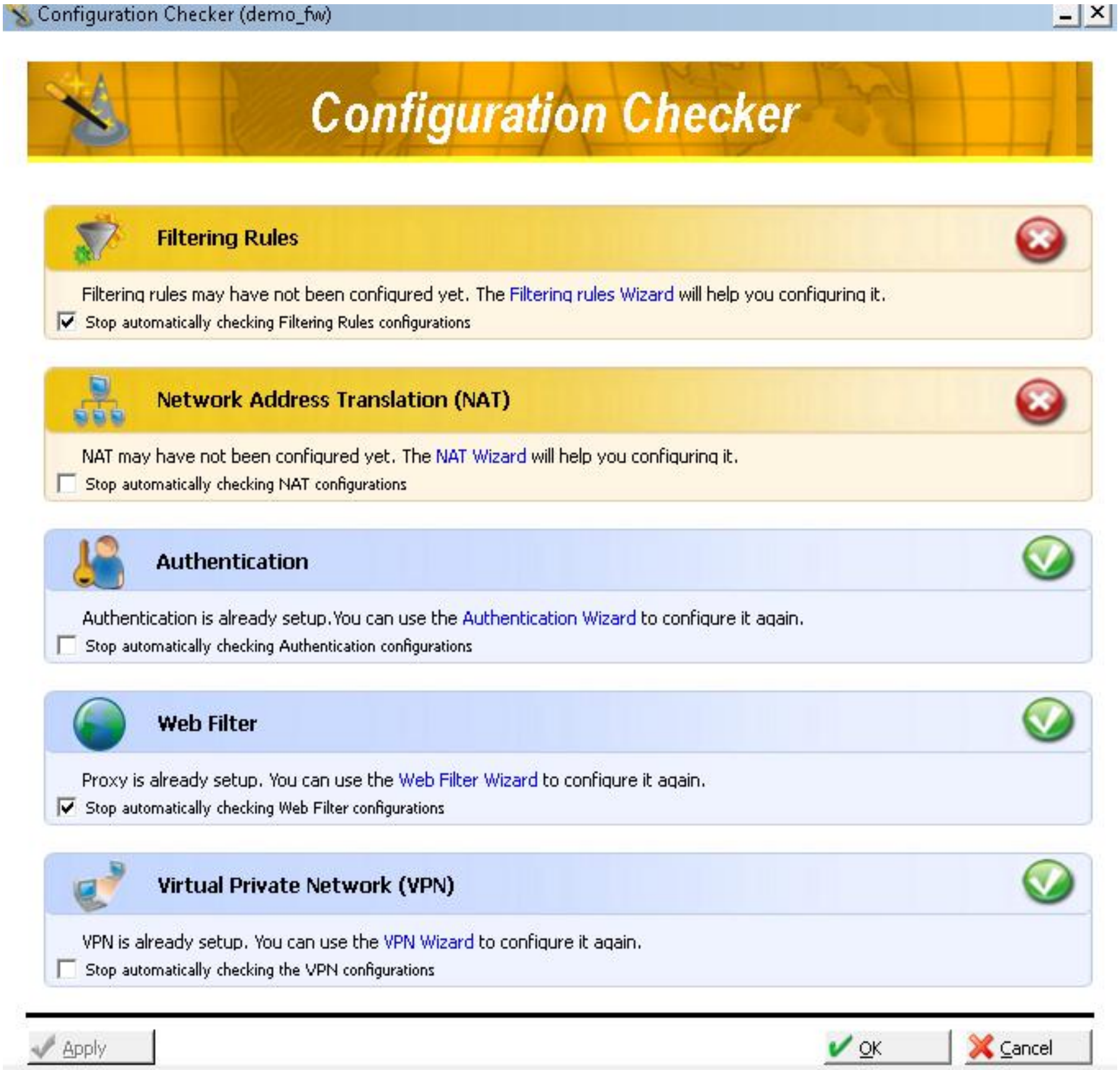


Image 46 – Connect Button.

It will connect the interface to the chosen firewall, as indicated on the Images below:



Configuration Checker (demo_fw)

Configuration Checker

Filtering Rules

Filtering rules may have not been configured yet. The Filtering rules Wizard will help you configuring it.

☑ Stop automatically checking Filtering Rules configurations

Network Address Translation (NAT)

NAT may have not been configured yet. The NAT Wizard will help you configuring it.

☐ Stop automatically checking NAT configurations

Authentication

Authentication is already setup.You can use the Authentication Wizard to configure it again.

☐ Stop automatically checking Authentication configurations

Web Filter

Proxy is already setup. You can use the Web Filter Wizard to configure it again.

☑ Stop automatically checking Web Filter configurations

Virtual Private Network (VPN)

VPN is already setup. You can use the VPN Wizard to configure it again.

☐ Stop automatically checking the VPN configurations

Image 47 – Interface connected to the chosen Firewall.

In case the administration session cannot be established, a window showing the error that stopped it from opening will be displayed. In this case, there are many possible messages. Listed below are the most common error messages:

- Aker is already being used by another interface;

Aker Firewall only allows the existence of one administration session at a time. If this message is displayed, it means that there already is another connected remote interface or a local administration module is already in use.

- Network error, connection shut down by server;

This is a generic error and may have a series of causes. Its most common cause is due to typing mistakes during login or password insertion. If user login is not registered or if the password is incorrect, the server will shut down the connection. First verify if login and password have been correctly typed in. In case the error persists, follow the steps described below:

1. Check if the user attempting to connect is registered in the system and if the password is correct (to do this, employ the user administration local module. Check the chapter entitled “***Administering firewall users”***).
2. Verify if the network is working properly. There are many possible ways to do this. One of them is using the *ping* command. (Do not forget to add a rule liberating ***‘echo request’*** and ***‘echo reply’*** *ICMP* services for the computer on which testing towards firewall, in case of ping use. To learn how this is done, see the chapter entitled ***“*Stateful Inspection”**). If this does not work, then the network has connectivity problems and this should be fixed before a remote administration is tried. In case it works, see step 3.
3. Verify the existence of a registered rule liberating access from the computer that wants the firewall connection, using Aker service (*TCP, port 1020*). In case it does not exist, insert this rule (to learn how this is done, read the chapter entitled ***“Stateful Inspection”***).

3.3. Ending remote administration

There are three ways to end remote administration on Aker Firewall:

End session by right-clicking the mouse on the connected firewall and selecting “***Disconnect from remote device”***

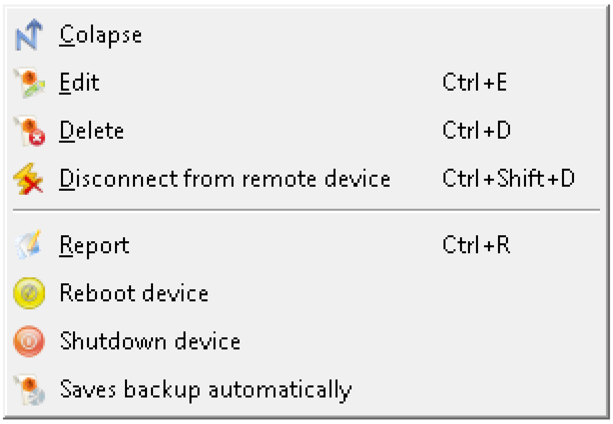

Colapse
Edit Ctrl+E
Delete Ctrl+D
Disconnect from remote device Ctrl+Shift+D
Report Ctrl+R
Reboot device
Shutdown device
Saves backup automatically

Image 48 – Ending Aker Firewall remote administration (Disconnecting from remote device).

Click on ***“Disconnect from firewall”*** on the Toolbar, or shut down the Remote Interface. In this case all firewall connections will be immediately lost.

In case you wish to exit the program, click the ***“Exit”*** option on the main window Toolbar or click the ***‘x’*** on the top right of the window.

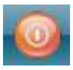


Image 49 – Button: Exit from this program.

3.4. Changing user passwords

It is possible for any Aker Firewall user to change his or her password as much as they need to. Therefore, it is necessary to establish an administrator session (as indicated in the topic ***"Starting remote interface"***) and after this, the steps below should be executed:

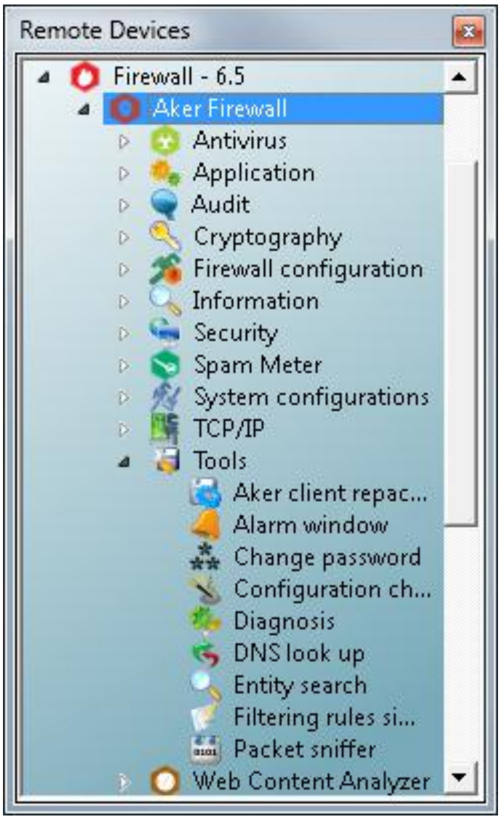

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repac...
Alarm window
Change password
Configuration ch...
Diagnosis
DNS look up
Entity search
Filtering rules si...
Packet sniffer
Web Content Analyzer

Image 50 – Remote Device (performing password change).

- Select the firewall to be configured;
- Click on ***Tools***;
- Select ***Change password***.

The following screen will be displayed:

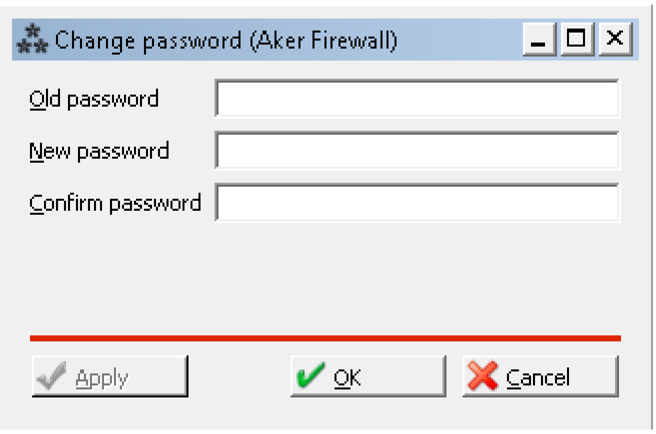

Change password (Aker Firewall)
Old password
New password
Confirm password
Apply
OK
Cancel

Image 51 – Redefine Password (first insert old password, next, the new one followed by its confirmation).

The password to be changed should be typed in the ***"Old Password"*** field and the new one typed in fields, ***"New password"*** and ***"Confirm password"*** (password will show on the screen as many asterisks '*').

After filling out these fields, hit ***'OK'*** to change the password or hit ***'Cancel'*** in case you do not want to change it.

The fields ***'Old password'***, ***'New Password'*** and ***'Confirm password'***, should contain from 6 to 14 characters.

3.5. Visualizing session information

At any moment it is possible to visualize certain information regarding active administration sessions. For this, there is a specific window containing useful information such as login, names and rights of user who is administrating the firewall along with the version and release of the Aker Firewall that is being administrated. It also shows the time that the connection was established and how long it has been active. To open this window, go through the following steps:

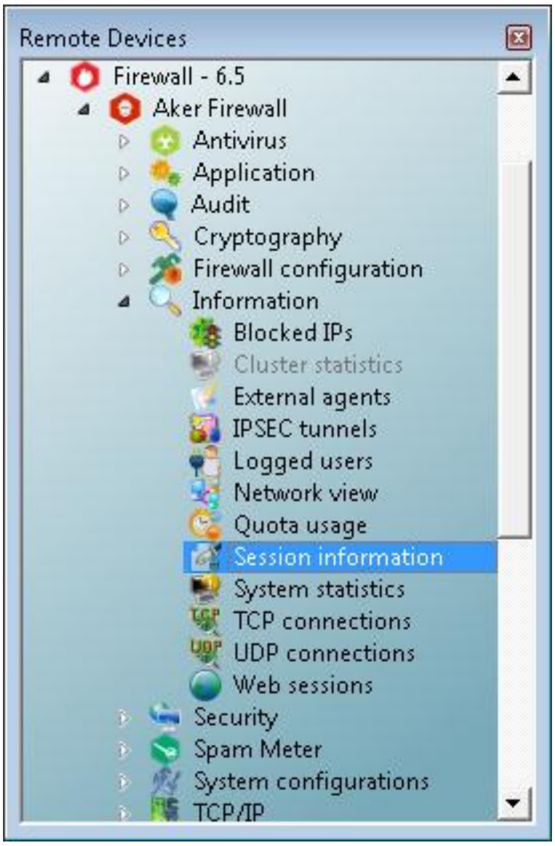
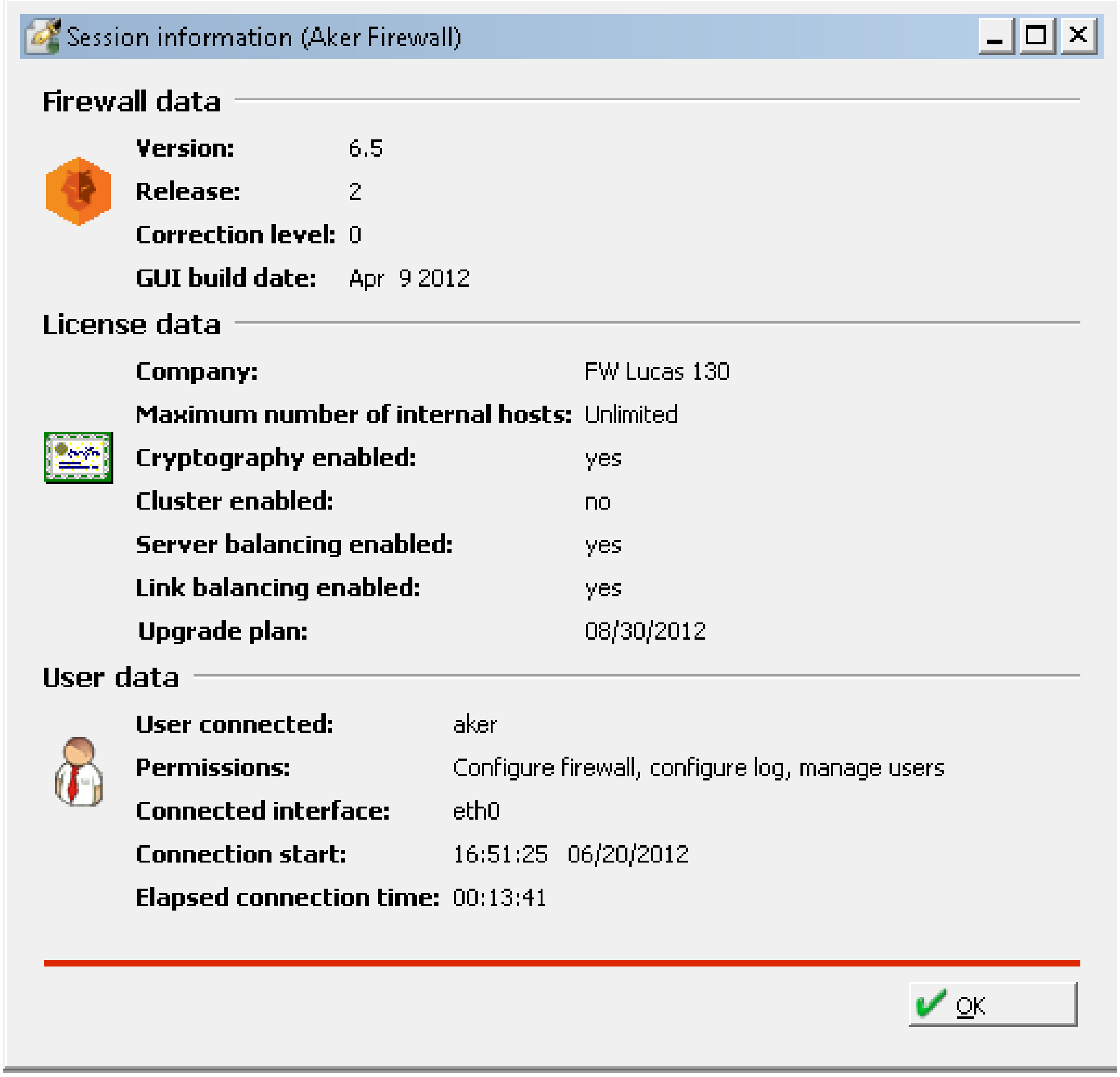

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP

Image 52 – Remote devices (Visualize session Information).

- Select the firewall to be configured;
- Click on the ***Information*** menu;
- Select ***Session Information***.

The following window will open:



Firewall data

Version: 6.5
Release: 2
Correction level: 0
GUI build date: Apr 9 2012

License data

Company: FW Lucas 130
Maximum number of internal hosts: Unlimited
Cryptography enabled: yes
Cluster enabled: no
Server balancing enabled: yes
Link balancing enabled: yes
Upgrade plan: 08/30/2012

User data

User connected: aker
Permissions: Configure firewall, configure log, manage users
Connected interface: eth0
Connection start: 16:51:25 06/20/2012
Elapsed connection time: 00:13:41

Image 53 – Session Information (reveals Firewall data, License data and Users data).

3.6. Using Remote Interface tools

What are Aker Firewall Remote Interface tools?

These tools are sets of utilities only available on Aker Firewall Remote Interface. Their function is to aid and favor the firewall administration, providing a series of useful functions on a day-to-day basis.

3.7. Activation Keys

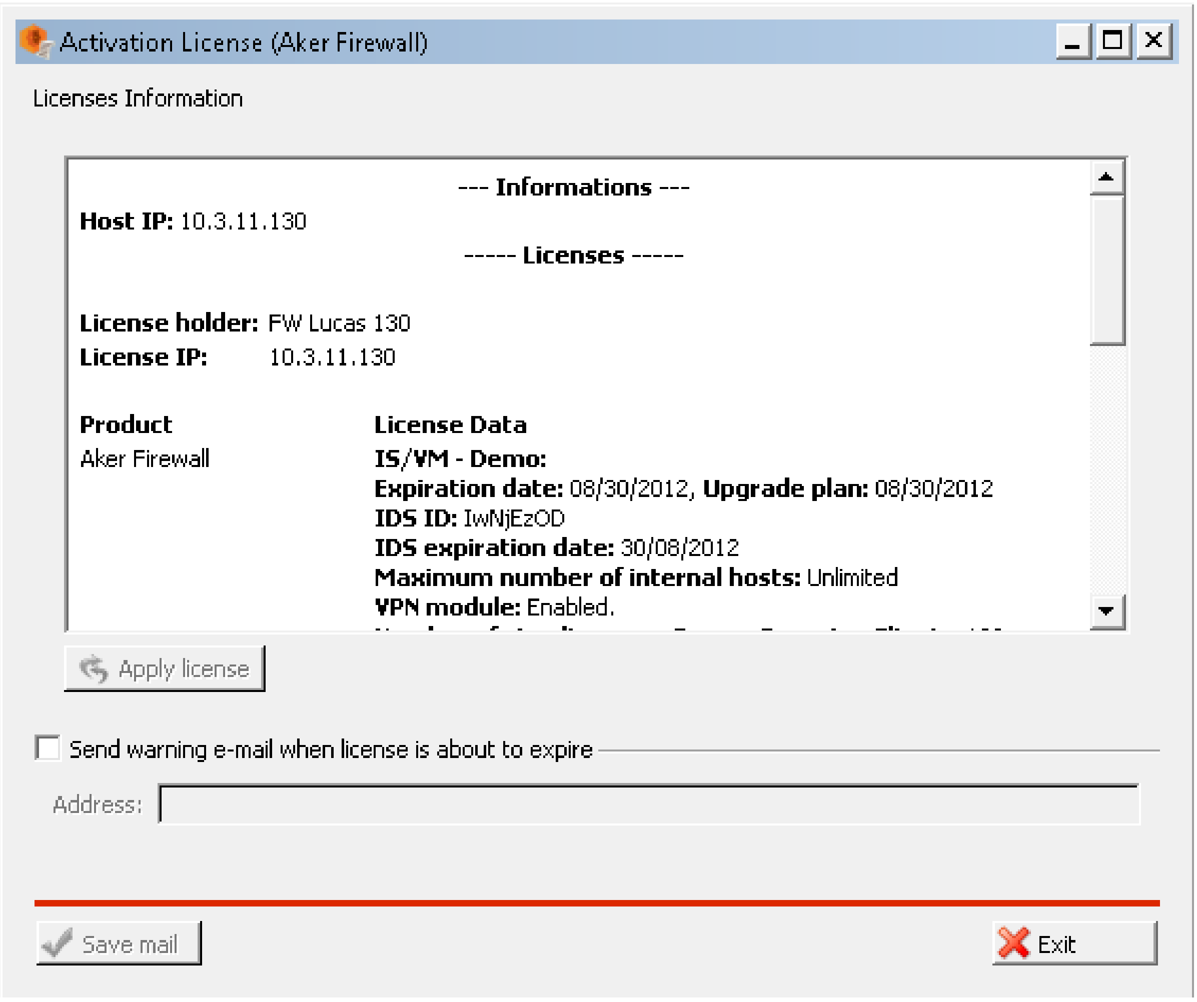
This option allows the updates of Aker Firewall activation key as well as updates of other products that may be installed together: Antivirus, Spam Meter, Secure Roaming and Web Content Analyzer.

To see or update the license:

Click on the ***"Load / Show license"*** button on the connected firewall task bar.

Image 54 – Button: Load / Show license.

Activation License window



Activation License (Aker Firewall)
Licenses Information
Apply license
Save mail
Exit

--- **Informations** ---

Host IP: 10.3.11.130

----- **Licenses** -----

License holder: FW Lucas 130

License IP: 10.3.11.130

Product	**License Data**
Aker Firewall	**IS/VM - Demo:** **Expiration date:** 08/30/2012, **Upgrade plan:** 08/30/2012 **IDS ID:** IwNjEzOD **IDS expiration date:** 30/08/2012 **Maximum number of internal hosts:** Unlimited **VPN module:** Enabled.

☐ Send warning e-mail when license is about to expire

Address:

Image 55 – Activation License information.

This is just an informative window. It features all products installed together with the firewall and the data related to the license of each respective product. Among this data, you can verify expiring dates, the number of licenses, ID and IDS expiring dates and so on, regarding to each product.

In case you wish to insert a new license, click on ***“Load”*** located on the taskbar. This option will open a dialog box with the file from where a new key will be loaded. In case of Firewall Box, if there is more than one product installed together with the firewall, the additional product keys are also used.

From Aker Firewall version 6.0 onwards it is no longer possible to update firewall activation keys by typing them, updates are only possible by loading them from the *file sent by Aker Security Solutions or one of its authorized representatives.*

3.8. Saving configurations (backup)

This option allows the firewall security configuration be completely saved on the computer where you are administrating. In case of a disaster, this configuration can posteriorly be easily restored.

To save these configurations, connect to a remote device and click the ***“Save backup of selected item”***:

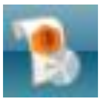
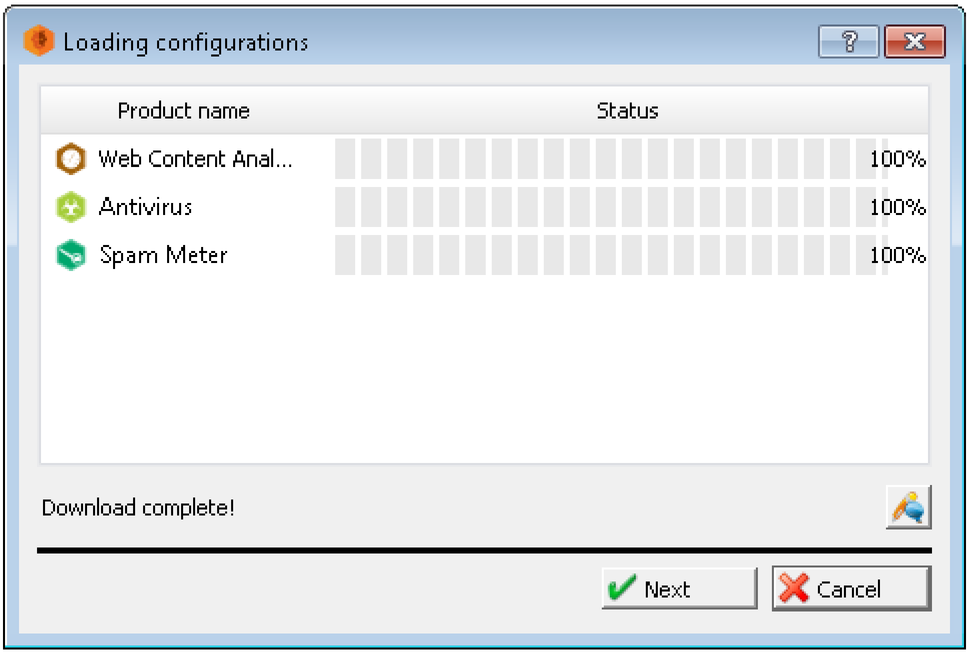


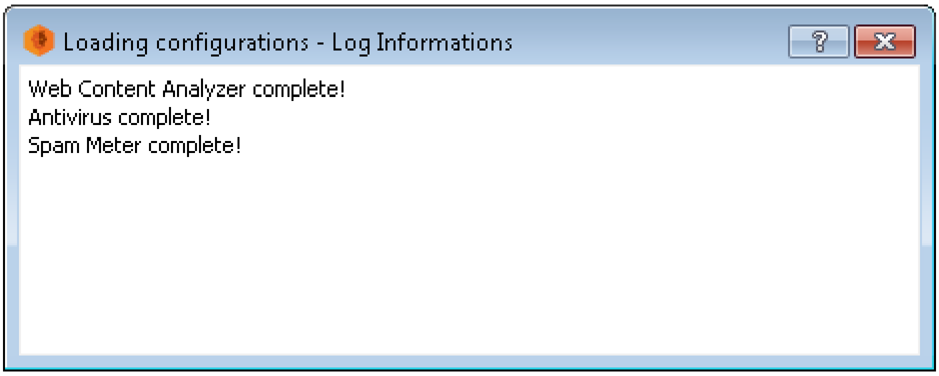
Image 56 – Button: Save backup of selected item.

Perform personalized configurations and products training bases downloads:


Loading configurations
Product name
Status
Web Content Anal...
100%
Antivirus
100%
Spam Meter
100%
Next
Cancel

Download complete!

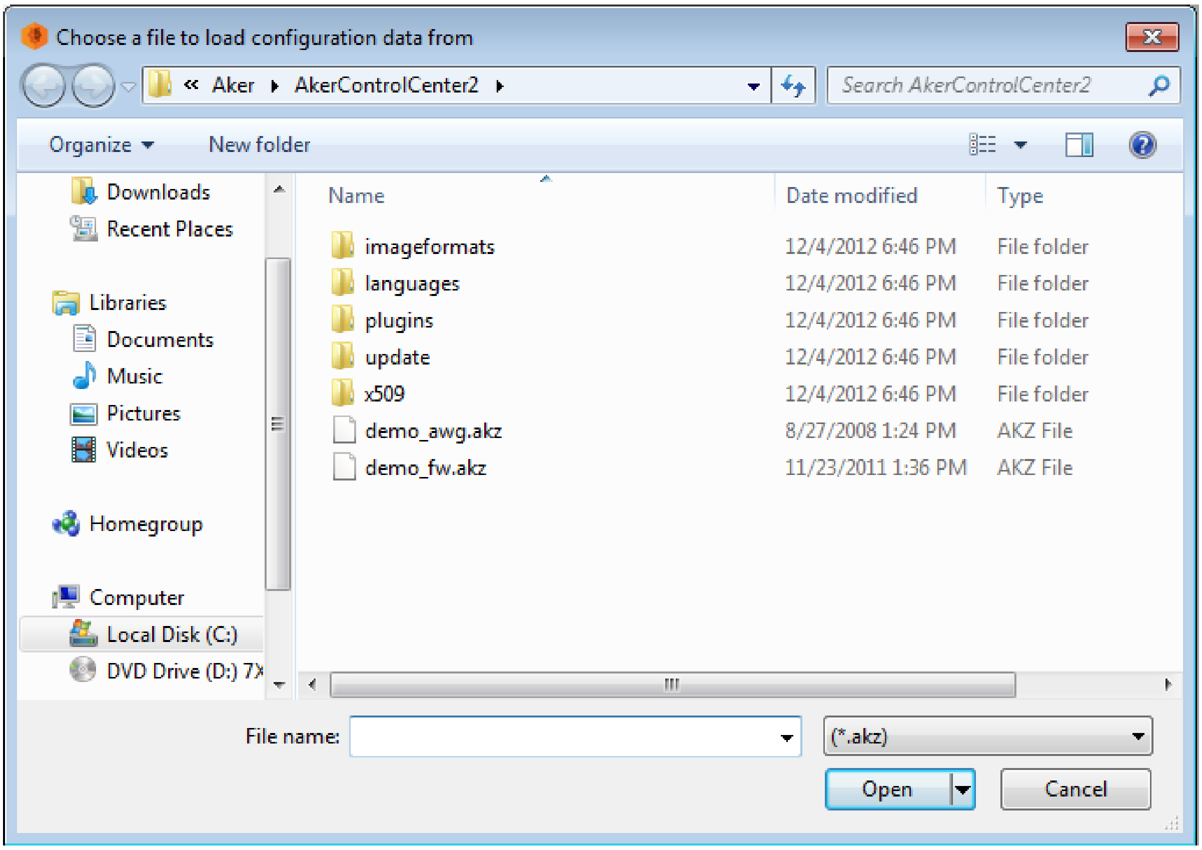
Image 57 – Personalized configurations and products training base downloads.


Loading configurations - Log Informations

Web Content Analyzer complete!
Antivirus complete!
Spam Meter complete!

Image 58 – Backup Log information.

The window to save configurations:


Choose a file to load configuration data from
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize ▾
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
File name:
(*.akz)
Open
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder
demo_awg.akz	8/27/2008 1:24 PM	AKZ File
demo_fw.akz	11/23/2011 1:36 PM	AKZ File

Image 59 – File selection screen to save configurations.

After typing the name of the saved file, click on ***"Save"***. In case the security copy is no longer desired, click on ***"Cancel"***.

This option allows the copy of the firewall security configuration completely through the previous option.

Automatically saves backup

Through the following configuration, a complete backup of the remote device is saved each time it automatically connects. To activate it select the option “***Save backup automatically”*** as indicated by the Image below:

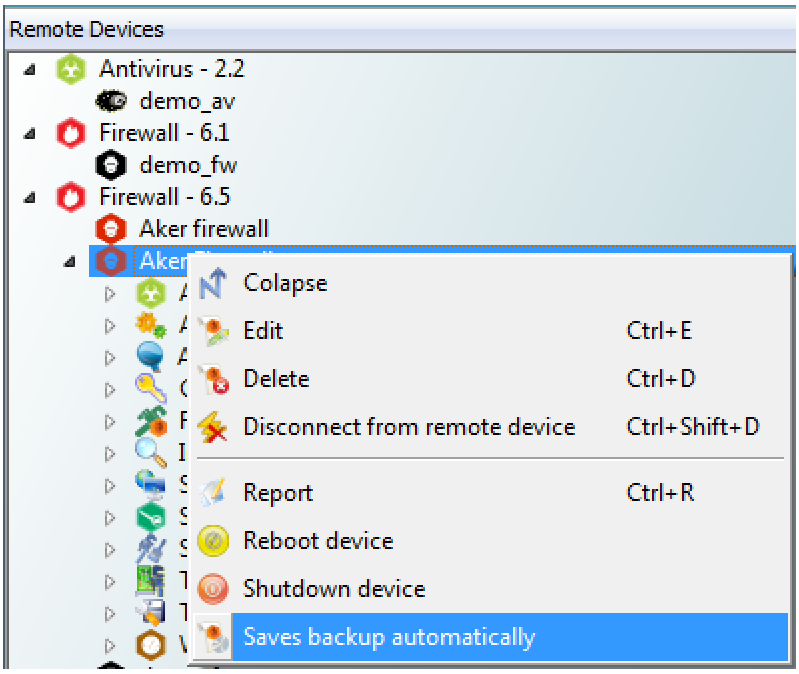

Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker firewall
Aker
Colapse
Edit Ctrl+E
Delete Ctrl+D
Disconnect from remote device Ctrl+Shift+D
Report Ctrl+R
Reboot device
Shutdown device
Saves backup automatically

Image 60 – Save backup automatically.

Backups are saved in the Aker Control Center installation folder.

3.9. Restore configurations

In order to restore a security copy, the following steps should be taken:

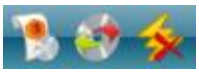


Image 61 – Buttons for the backup restore.

- Click on the firewall on which the security copy will be loaded.
- Select the item ***“Load configurations”*** on the taskbar or on the menu with the selected firewall name:

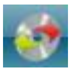
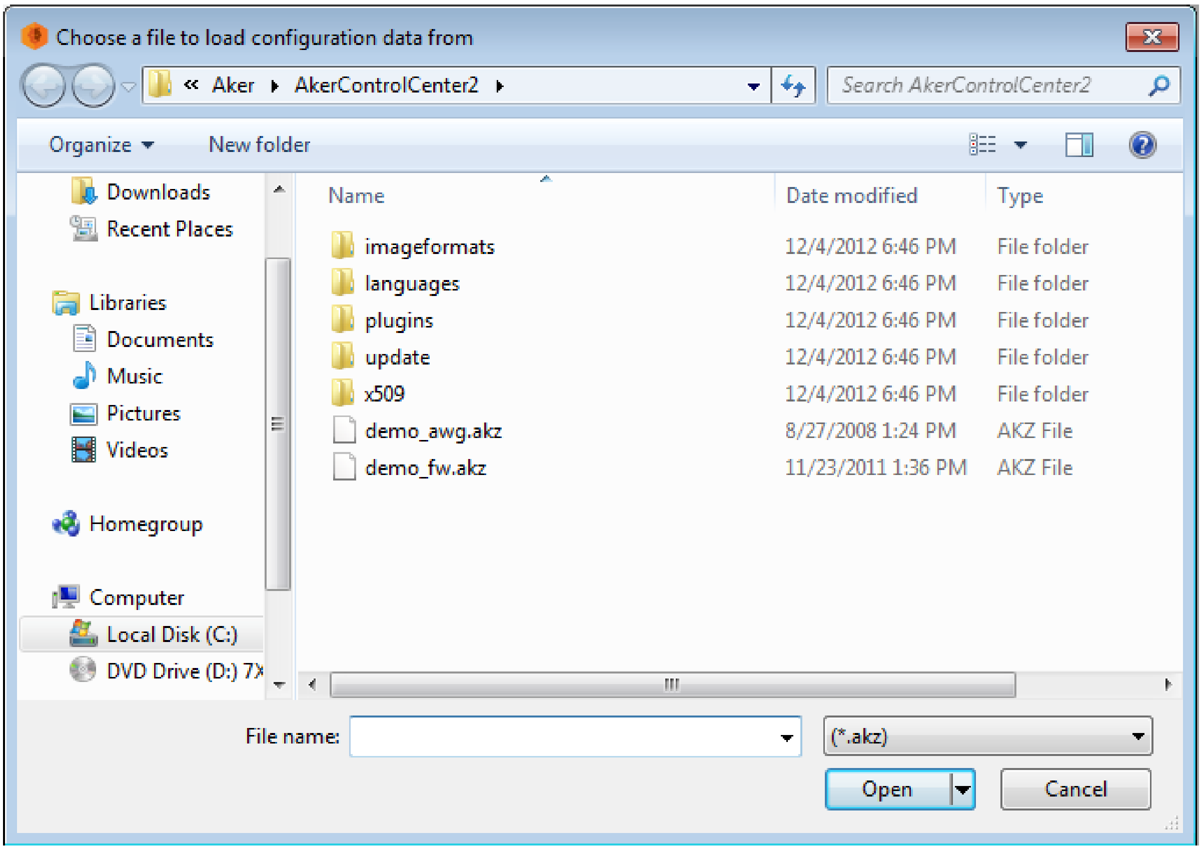


Image 62- Button: Loads file backups.

The window to load configurations:



Choose a file to load configuration data from
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize ▾
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
File name:
(*.akz)
Open
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder
demo_awg.akz	8/27/2008 1:24 PM	AKZ File
demo_fw.akz	11/23/2011 1:36 PM	AKZ File

Image 63 – File selection to load configuration data.

This window allows the user to choose the file name where the configuration will be restored. After specifying its name, the firewall will read all of its contents, perform many consistency tests and if the content is valid it will be loaded.

- The ***"Open"*** button will load the copy and the update the firewall configuration immediately.
- The ***"Cancel"*** button will close the window; however the security copy will not be loaded.

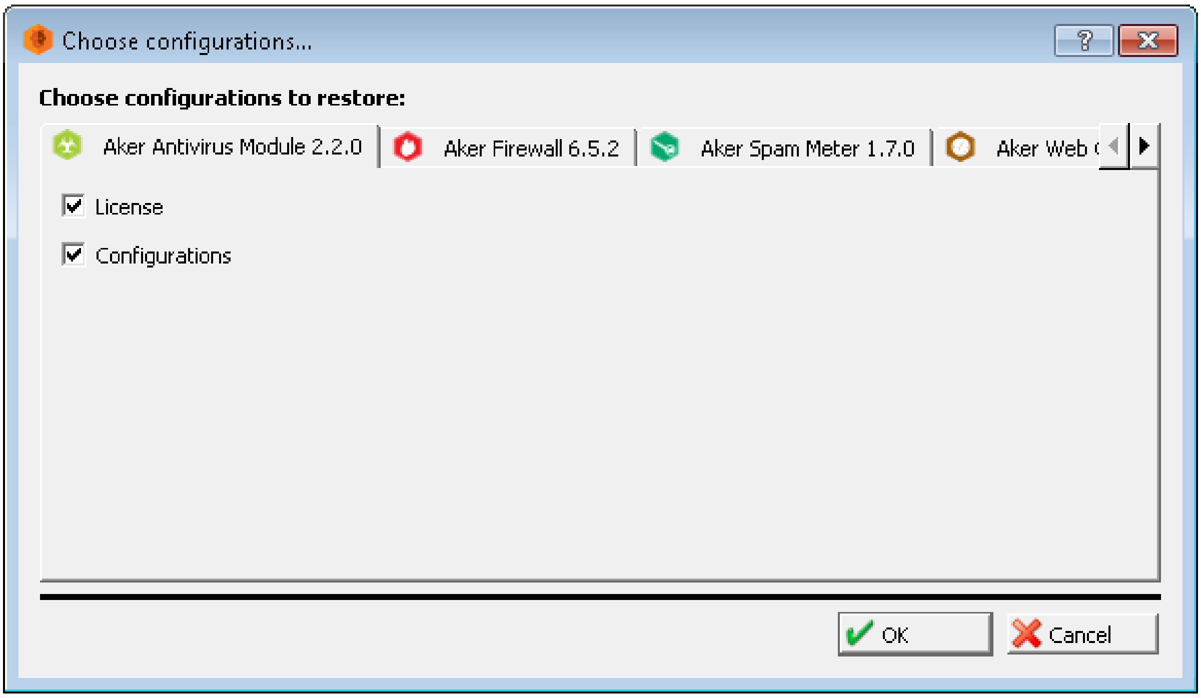
It is possible to choose, at the time of backup restoration, which configuration will be applied to the product, grouped by similarity.

Example:

- Rules;
- License;

- Certificates;
- Temporary data base;
- TCP/IP;
- Access profiles.

Being possible to select them from the following windows:

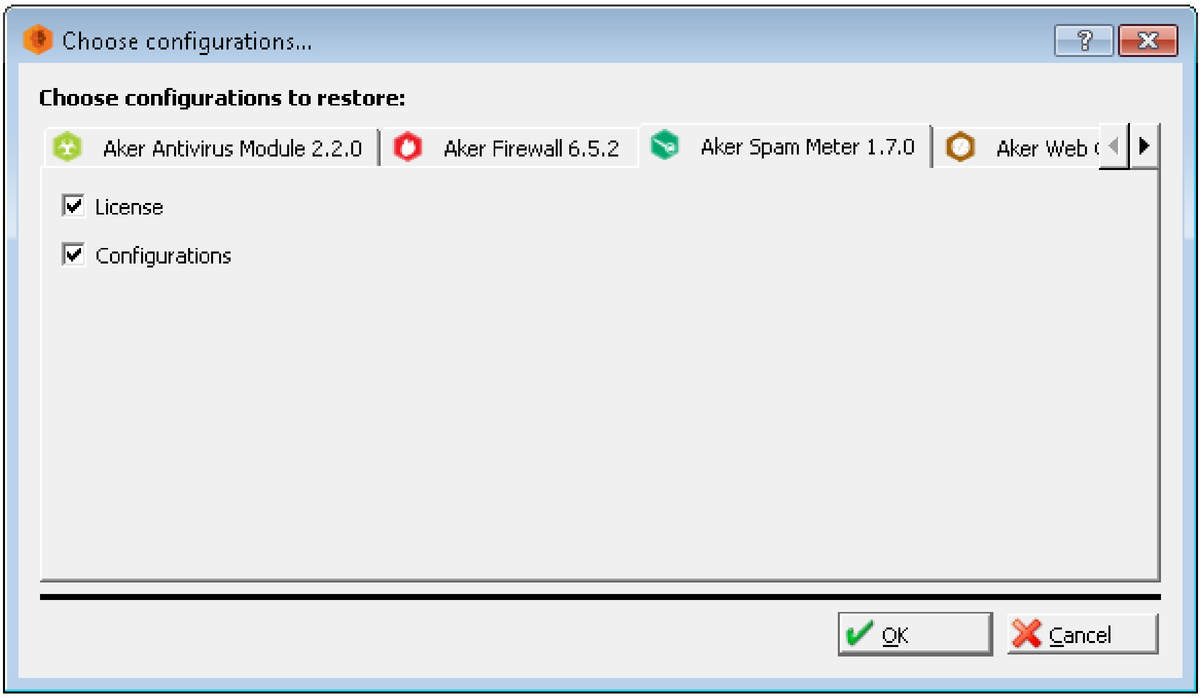

Choose configurations...
Aker Antivirus Module 2.2.0
Aker Firewall 6.5.2
Aker Spam Meter 1.7.0
Aker Web (
OK
Cancel

Choose configurations to restore:

☑ License

☑ Configurations

Image 64 – Antivirus module backup restore.


Choose configurations...
Aker Antivirus Module 2.2.0
Aker Firewall 6.5.2
Aker Spam Meter 1.7.0
Aker Web (
OK
Cancel

Choose configurations to restore:

☑ License

☑ Configurations

Image 65 – Aker Spam Meter backup restore.

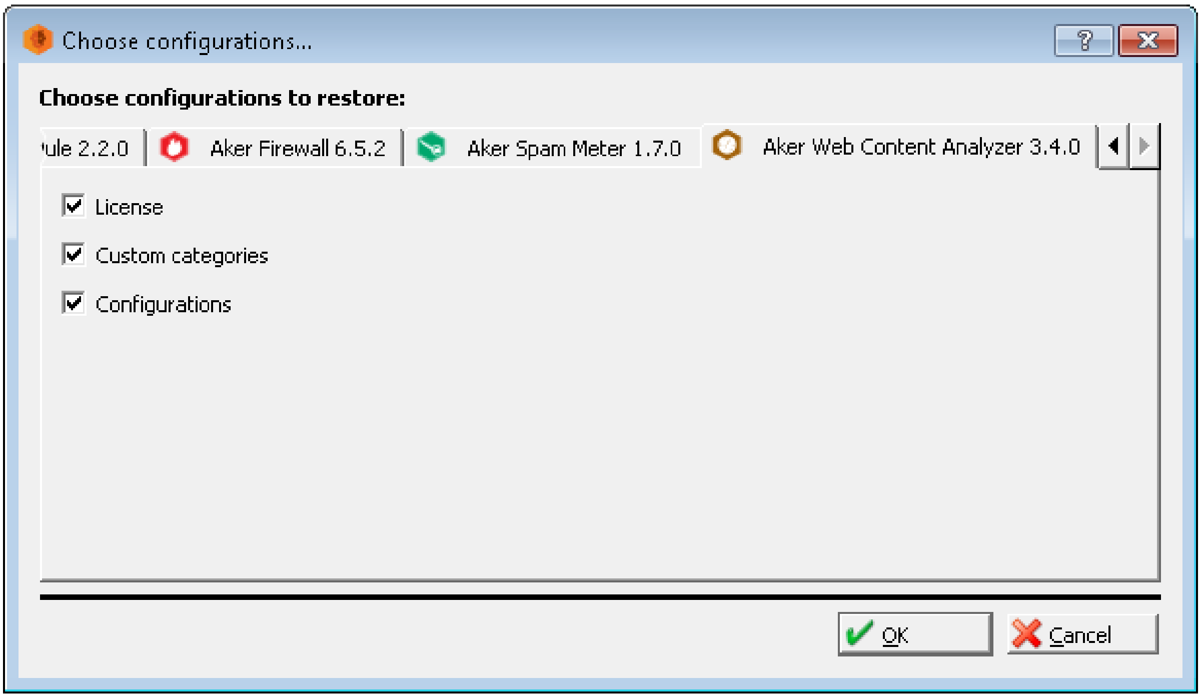

Choose configurations...
Choose configurations to restore:
ule 2.2.0
Aker Firewall 6.5.2
Aker Spam Meter 1.7.0
Aker Web Content Analyzer 3.4.0
☑ License
☑ Custom categories
☑ Configurations
OK
Cancel

Image 66 – Web Content Analyzer backup restore.

The system version will be displayed as of backup generation and alerts may be displayed in case of incompatibility.

3.10. Restarting the Firewall

This option is used to restart the firewall; however it should not be used under normal operational conditions. The only operation that requires the firewall restart is the load of an external encryption algorithm.

To restart the firewall:

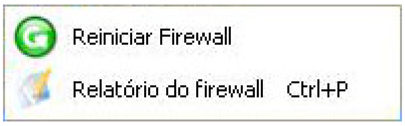

Reiniciar Firewall
Relatório do firewall Ctrl+P

Image 67 – Restart the Firewall.

- Select the ***'Restart Firewall'*** item on the menu with the option ***'Firewall Actions'***.

3.11. Updates

What are updates and how to get them?

Like any other software, Aker Firewall may eventually present bugs in its operation. As these issues are solved, Aker produces a file which allows your Aker Firewall to be updated and the bugs fixed. Sometimes, certain new characteristics are added to an existing version, in a way that it increases its performance or flexibility.

In both cases the update or correction files are available free of charge on Aker website: just search the ***'Download'*** menu and select the options ***'Patches'*** and ***'Updates'***. These files are always cumulative, it is necessary to download only the last version and it will include the corrections present on the previous Patch/update files.

The update Window

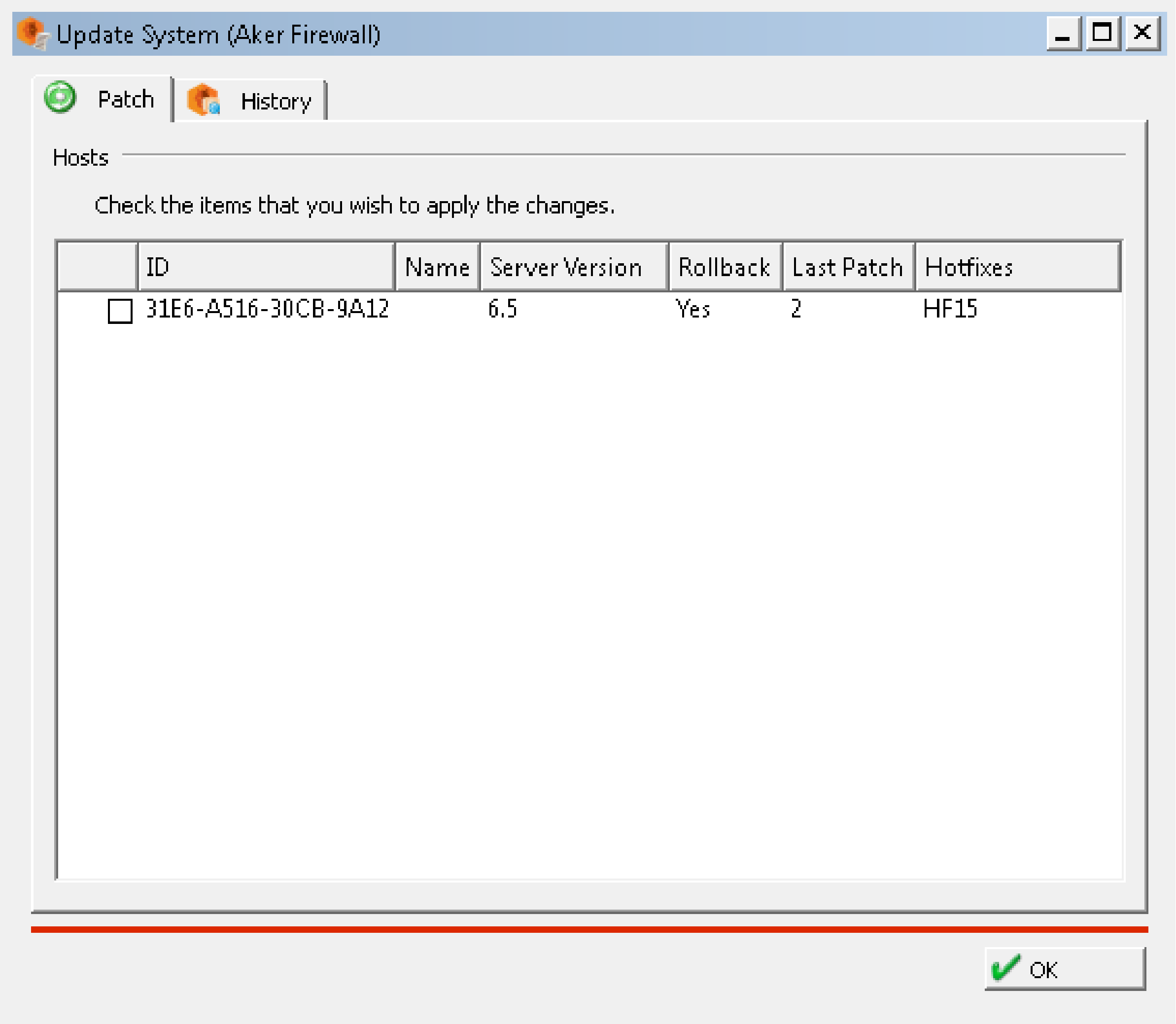
This option allows the remote application of an Aker Firewall patch or update, via Remote Interface. It is also possible to completely update the product version.

To gain access to the update window, the icon located on the toolbar should be clicked on, and then the window will be automatically opened so the updates may be selected and applied.

Image 68 – Button: Updates.

This window is divided into two tabs: ***'Patch'*** and ***'History'*,** as explained below:

Patch tab



Check the items that you wish to apply the changes.

	ID	Name	Server Version	Rollback	Last Patch	Hotfixes
☐	31E6-A516-30CB-9A12		6.5	Yes	2	HF15

Image 69 – Firewall data updating System.

Through this window is possible to visualize the current status of updates/corrections applied to Web Gateway. In case of cluster, the window will present the information of the computer composing it. It has the following fields:

Id: Refers to the identification of computers that composes the cluster.

Name: Refers to the name assigned to computers.

Restoration: This field informs whether the last update applied can be undone.

Updates applied through Patches and Hotfixes are changes that can be undone. This option allows the last update applied to the computer to be undone, whether it is hotfix or patch. Shall be observed that the changes are undone one by one, meaning, if the version is already on Patch 3, and the initial version is desired back, patch 3 should be undone, after this patch 2 should be undone, and so on.

Last update: Identification of the last patch applied to the cluster.

Hotfixes: List of hotfixes applied within the patch. On this list, the direct order of hotfix applications is displayed.

Hotfix is a small update or correction made for a specific patch. It can be applied independent from order, which does not happen to patch that should be applied in the sequential update order.

In the update or correction is destined to a different version of operating system or Aker Web Gateway version, then the “Apply” button will be disabled and the application will not be allowed.

To load an update/correction file, click on the icon below.

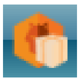
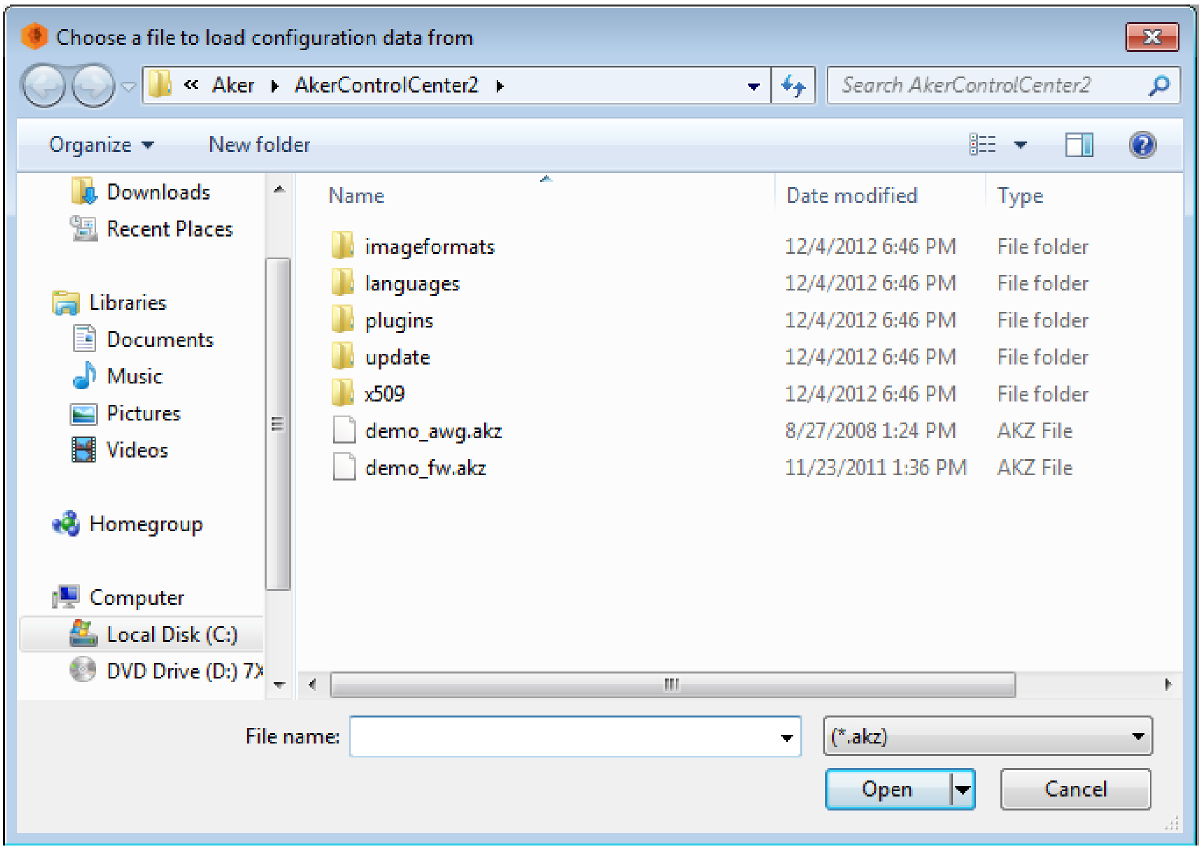


Image 70 – Button: Load update file.

Next a window allowing a patch or hotfix update file will open, as it is displayed in the image below.


Choose a file to load configuration data from
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize ▾
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
File name:
(*.akz)
Open
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder
demo_awg.akz	8/27/2008 1:24 PM	AKZ File
demo_fw.akz	11/23/2011 1:36 PM	AKZ File

Image 71 – Selecting the file to be updated /corrected.

To apply the update/patch file, the computer should be selected on the Patch tab, immediately after this the icon which the patch or hotfix will be applied should be clicked on.

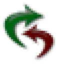


Image 72 – Apply patch or hotfix.

In case you wish to apply the rollback, at least one computer should be selected on the Patch tab, clicking the icon right after this, so these changes are undone one by one, in the sequence they were updated.

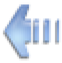
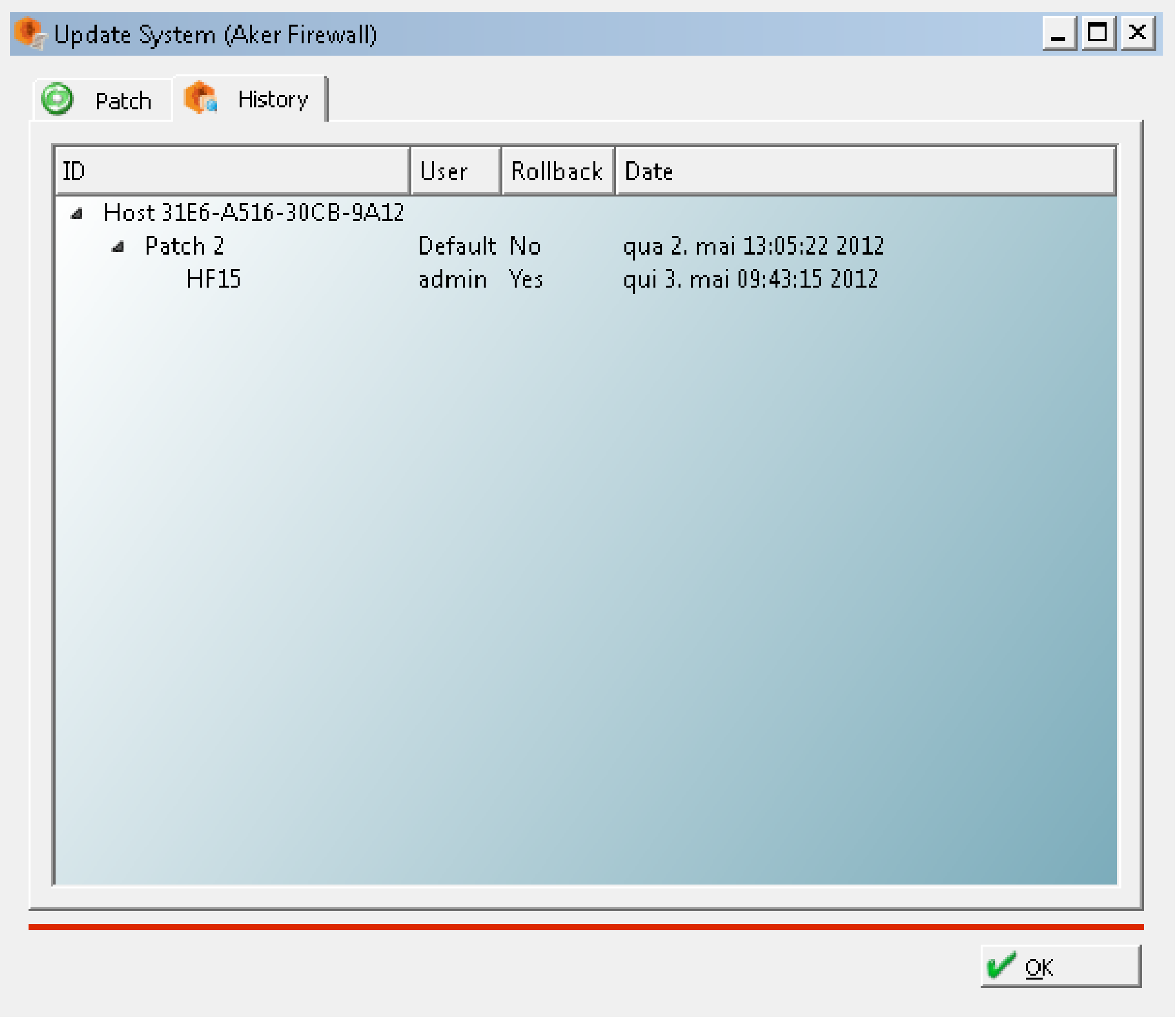


Image 73 – Apply rollback.

To apply rollback to more than one computer at the same time, these computers shall contain the same updates, for instance: all of them have patch 3 version, and want to go back to patch 1.

History Tab



ID	User	Rollback	Date
Host 31E6-A516-30CB-9A12			
Patch 2	Default	No	qua 2. mai 13:05:22 2012
HF15	admin	Yes	qui 3. mai 09:43:15 2012

Image 74 – Visualizing patch and hotfix historical applications.

This tab allows patch and hotfix history applications to be visualized.

The tab is composed by the following fields:

ID: Shows the computer identification from where the update was performed.

User: Indicates the user who applied the update.

Rollback: Indicates whether or not the update can be undone.

Date: Indicates the date when any patch or hotfix application was performed.

The expression "***Current Version***" means no patch has been applied.

Attention: By clicking the *"**OK**"* button, the Patch or Hotfix are not applied, just the window is closed.

3.12. Automatic Update Module – Aker Update System (AUS)

Aker Update System – **AUS** has the function of making available the update packets of all Aker products in the **Aker Control Center** directory. The system works in a smart way, where it will only bring the latest version for packets integrated to Aker Control Center, the latest Patches and Hotfixes.

Access to configuration windows

There are 3 ways of configuring the Update Module:

First option:

Select the desired Aker product

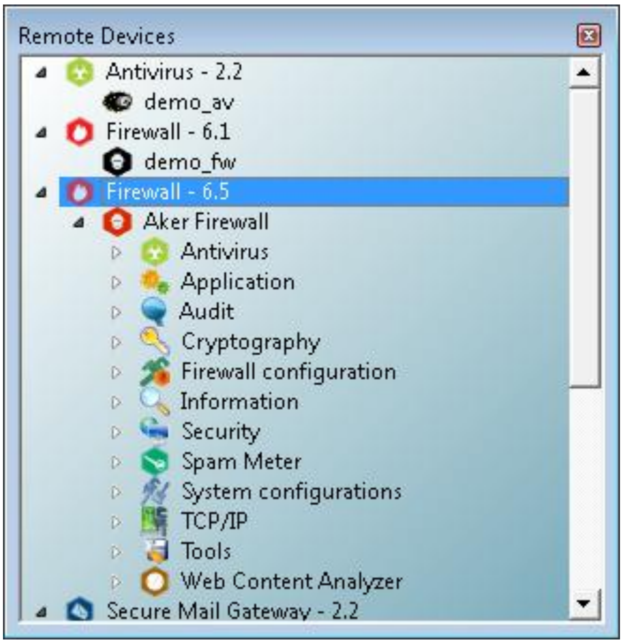
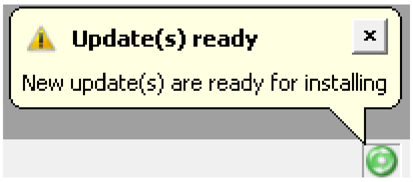

Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Secure Mail Gateway - 2.2

Image 75 – Accessing Aker Firewall

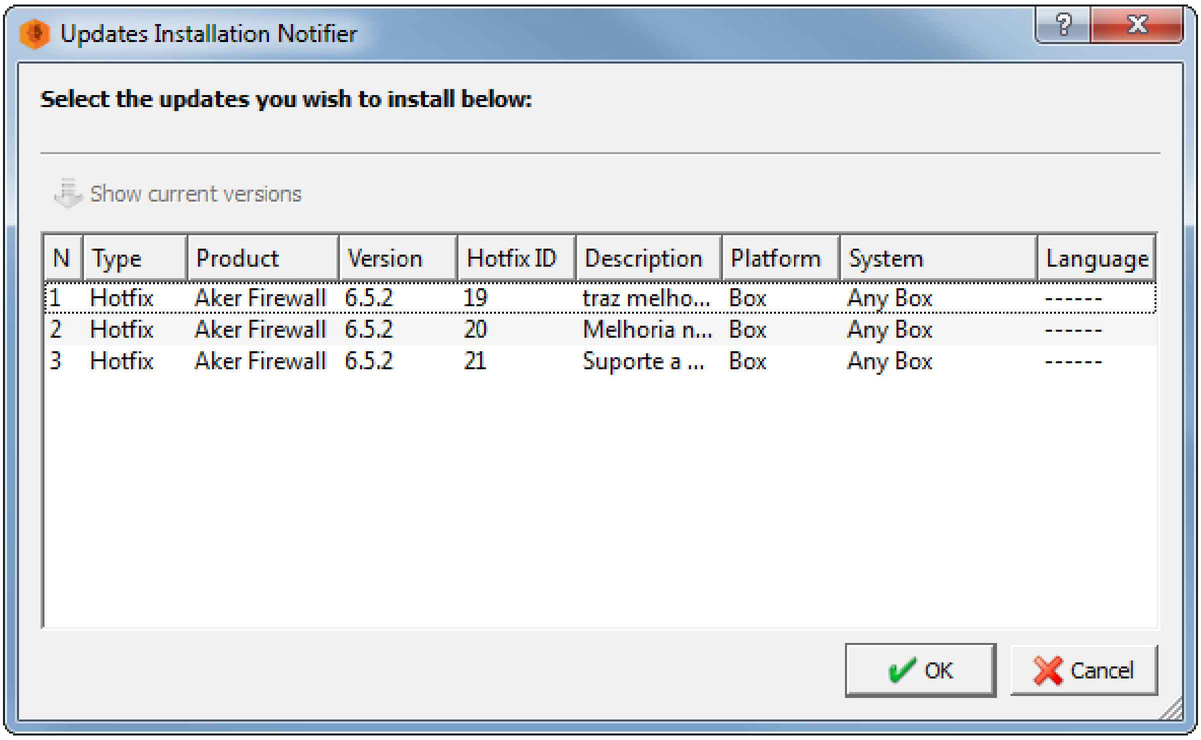
In case of an update is available, the following notification will show up on the lower right corner of the Control Center screen: **“Update(s) ready”.**


Update(s) ready

New update(s) are ready for installing

Image 76 – Notification of available updates on Aker Update System.

Left-click on the message and the **“Update Installer Notifier”** screen will show up. Updates to be installed should be chosen individually, then click on the **“OK”** button**.**


Updates Installation Notifier
Select the updates you wish to install below:
Show current versions
OK
Cancel

N	Type	Product	Version	Hotfix ID	Description	Platform	System	Language
1	Hotfix	Aker Firewall	6.5.2	19	traz melho...	Box	Any Box	------
2	Hotfix	Aker Firewall	6.5.2	20	Melhoria n...	Box	Any Box	------
3	Hotfix	Aker Firewall	6.5.2	21	Suporte a ...	Box	Any Box	------

Image 77 – Visualizing available updates through Aker Update System.

After this, the following screen will appear **“Update System”**. On *patch* it is possible to indicate the items which the changes and PT information will be applied (the description part informs what each one them corresponds). Just choose the best option and click **“OK”**. The update will be performed automatically, in case another update is required, repeat the procedure above.

Second option:

Select the desired Aker product

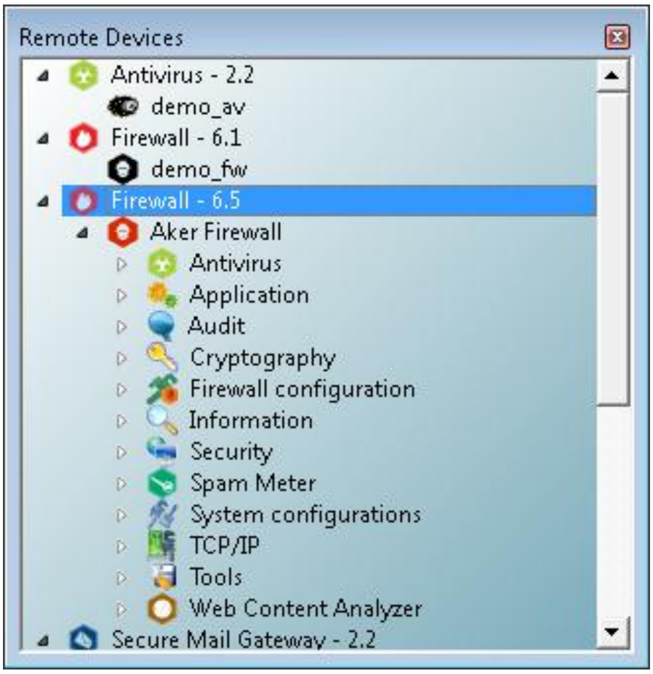

Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Secure Mail Gateway - 2.2

Image 78 – Accessing Aker Firewall

Click on the **"Updates"** button located on the Control Center screen's lower right corner and select one of the two following options: **"Updates to install"** or **"Updates to download".**

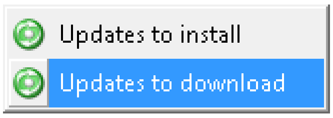

Updates to install
Updates to download

Image 79 – Accessing Aker Update System window

Third option

Select the desired Aker product

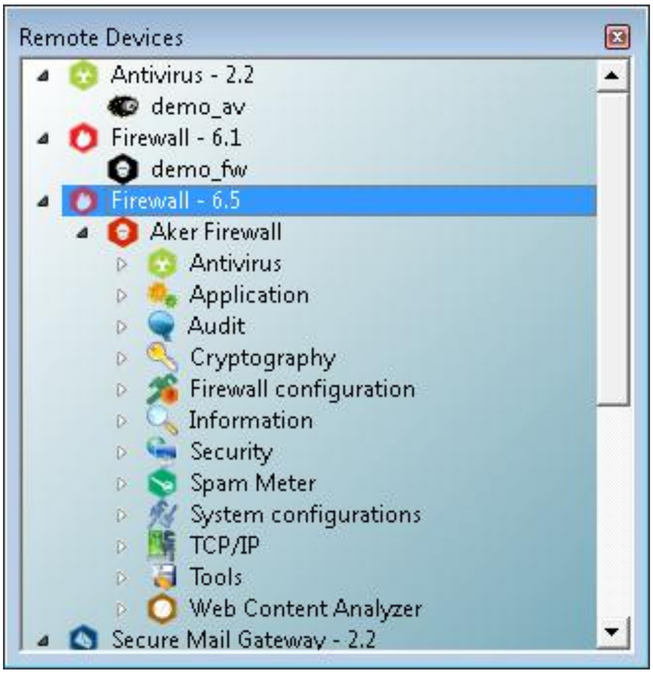

Remote Devices
Antivirus - 2.2
demo_av
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Secure Mail Gateway - 2.2

Image 80 – Accessing Aker Firewall

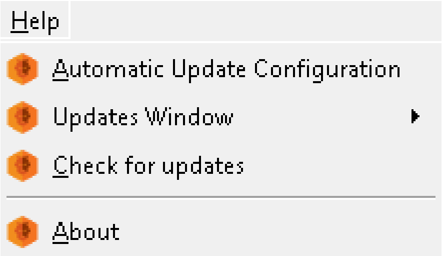

Help
Automatic Update Configuration
Updates Window
Check for updates
About

Image 81 – Help menu

Click on the **“Help”** icon and select one of the following three options:

- **“Automatic Update Configuration”:** updates will be performed constantly as of stipulated time;
- **“Updates Window”:** offers the option to open **“Download Window”** or **“Installation Window”.**
- **“Check for updates”**:

3.13. DNS Look up

DNS look up is used to solve computer names from their IP addresses. *Aker Firewall DNS look up* resolution window is used to provide address resolutions without needing to use additional programs.

Gaining access to the *DNS look up* window:

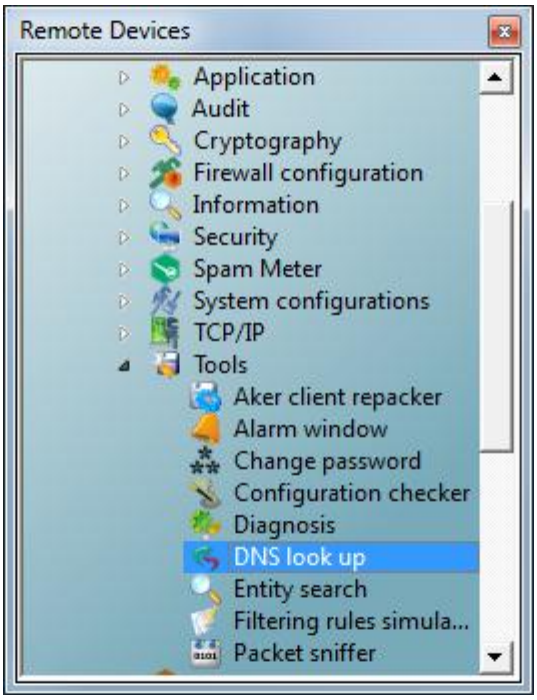

Remote Devices
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simula...
Packet sniffer

Image 82 – Reverse DNS window.

- Click on the firewall administration *Tools* menu.
- Select *DNS look up*.

DNS look up resolution window

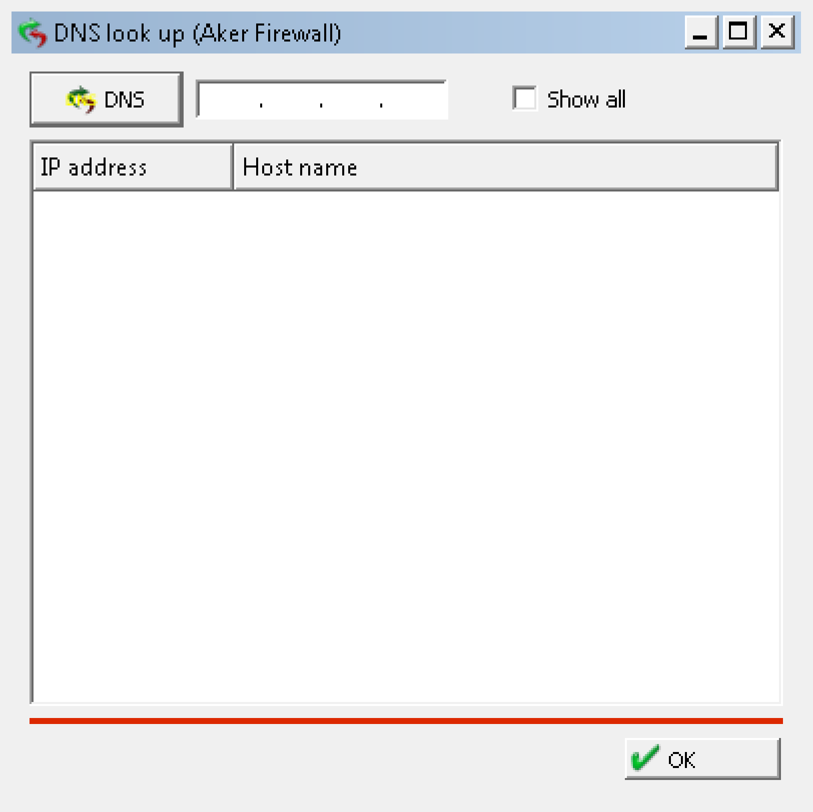


Image 83 – Reverse DNS

This window consists of a field to type in the IP address that needs resolving as well as a list of previously resolved IP addresses:

- If the “**Show all”** option is checked, all addresses that have been resolved will be displayed on the lower part of the window.
- The “**OK”** will close the window.

To resolve an address, type it in the field and click on the “**DNS”** button. At this moment the address will be displayed on lower window list, along with the resolution *status*. After some time, either the name of the corresponding computer will be show or an indication that the address informed does not have a configured DNS look up.

3.14. Filtering Rules Simulation

The Rule scans allow the administrator to test firewall rule configurations through a simulation of connection attempts. By analyzing the simulation results, it is possible to verify if the firewall is blocking the connections that should not be accepted and granting passage to those that should have it.

To gain access to the scanning window:

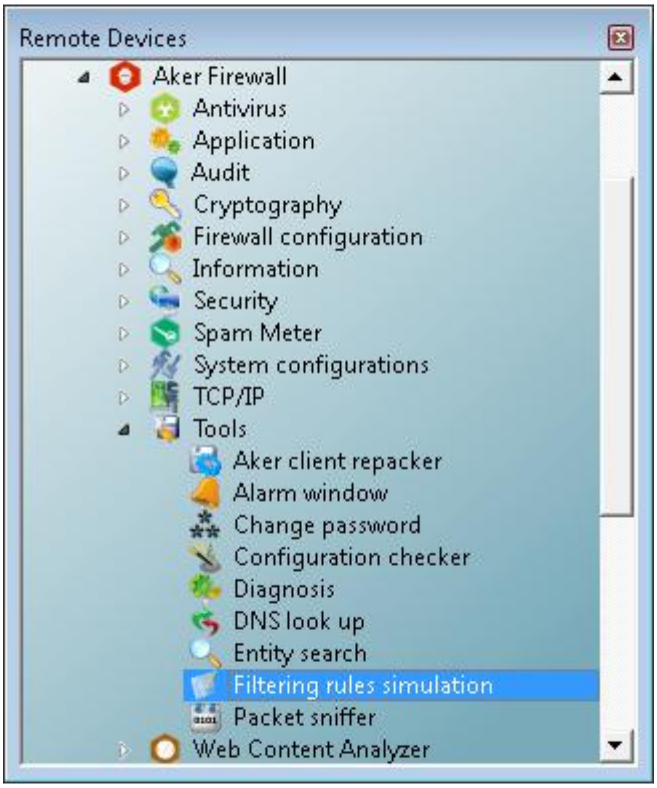

Remote Devices
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer
Web Content Analyzer

Image 84 – Access window to Filtering Rules Simulation.

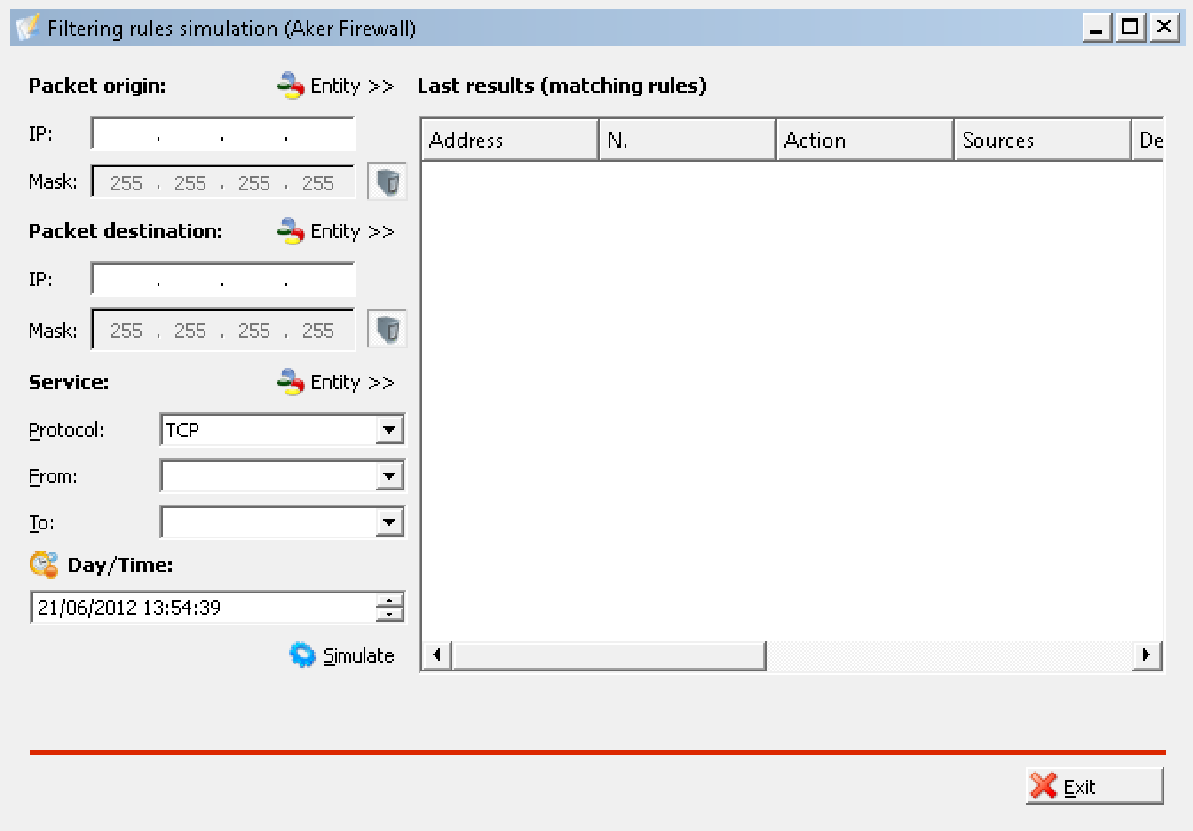
- Click on the firewall administration window > *Tools menu*.
- Select the **“Filtering Rules Simulation”**.

Filtering Rules Simulation

It is possible to switch between IP address scans and scans entities. Entity scanning is useful when all networks and services used have already been registered on the system. IP address scanning is most indicated when networks and services that are not or do not want to be registered on the system (external computers that will not be used in any filtering rules, for instance).

It is possible to either select the information for "*Packet origin*", "*Packet destination*" and "*Service*" from listed entities or type them in. To switch between the two operations modes, just click the related icons on the left of each of these fields.

- **Filtering Rules Simulation:** When the **IP address scanning option** is selected, the scanning window will have the following format:


Filtering rules simulation (Aker Firewall)
Packet origin:
Entity >>
Last results (matching rules)
Address
N.
Action
Sources
De
Packet destination:
Entity >>
Service:
Entity >>
Day/Time:
Simulate
Exit

IP: . . .

Mask: 255 . 255 . 255 . 255

IP: . . .

Mask: 255 . 255 . 255 . 255

Protocol: TCP

From:

To:

21/06/2012 13:54:39

Image 85 – Filtering Rules Simulation (packet origin, date, time and masks).

The "**IP**" and "**Mask**" fields inside ***Packet origin*** specify the range of computers used as source of simulated connections. The "**IP**" and "**Mask**" fields inside ***Packet Destination*** specify the range of computers used as destination of simulated connections.

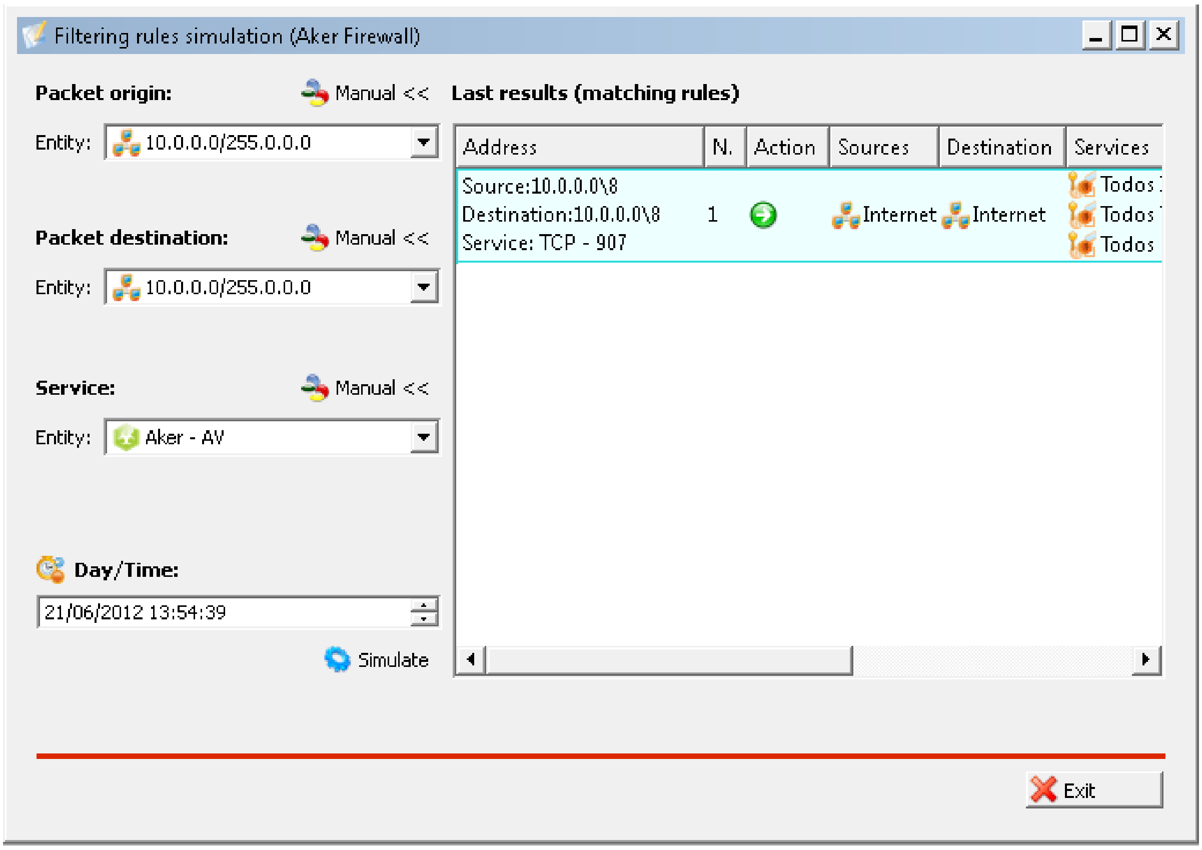
The "**Service**" field specifies the protocol and the range of simulated ports.

In case of TCP and UDP protocols, service values are destiny ports; in case of ICMP it is the type of service; and in case of other protocols, the protocol's value.

The “**Day/Time”** field allows the administrator to test the rules for a day of the week and time.

- **Scanning Entities**

Filtering Rules Simulation: When the **Entity scanning option** is selected, the scanning window will have the following format:



Packet origin:

Entity: 10.0.0.0/255.0.0.0

Packet destination:

Entity: 10.0.0.0/255.0.0.0

Service:

Entity: Aker - AV

Day/Time:

21/06/2012 13:54:39

Last results (matching rules)

Address	N.	Action	Sources	Destination	Services
Source:10.0.0.0\8 Destination:10.0.0.0\8 Service: TCP - 907	1	→	Internet	Internet	Todos Todos Todos

Image 86 – Filtering Rules Simulation (packet origin, packet destination, date, time and entity).

The **“Packet origin”** allows specifying the entity to be used as source of simulated connections.

The **“Packet Destination”** allows specifying in what entity the connections have to go to.

The **“Service”** allows specifying the protocol and the range of ports to be simulated through an entity.

The **“Day/Time”** allows the administrator to test the rules for a day/time of the week

Only one source entity, destination entity and service may be selected at once.

3.15. Reports

This option enables the administrator to print a full (or partial) report of the firewall configuration in a fast and easy way. This report is extremely useful for documentation purposes or configuration analysis.

To gain access to the reports widow:

- On the *toolbar*, click on the remote device which the report generation is needed and select the **"Report"** option.

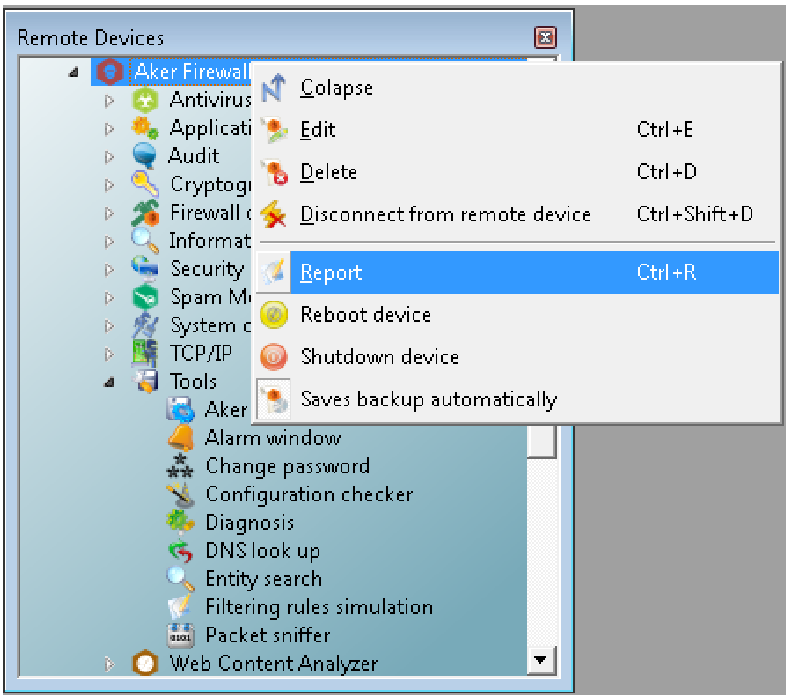

Remote Devices
Aker Firewall
Antivirus
Applicati
Audit
Cryptogr
Firewall c
Informat
Security
Spam M
System c
TCP/IP
Tools
Aker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer
Web Content Analyzer
Colapse
Edit Ctrl+E
Delete Ctrl+D
Disconnect from remote device Ctrl+Shift+D
Report Ctrl+R
Reboot device
Shutdown device
Saves backup automatically

Image 87 – Access window: Report.

The Report window

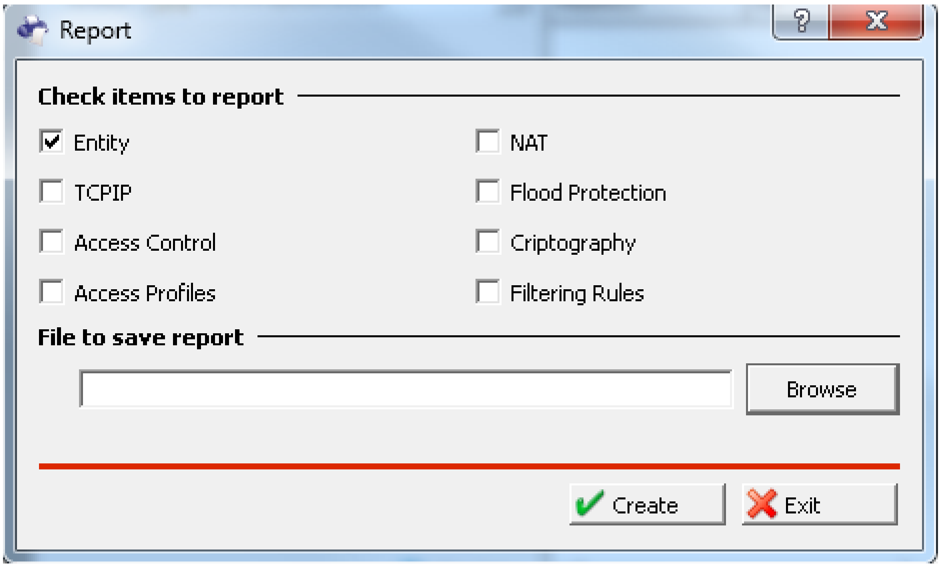

Report
Check items to report
☑ Entity
☐ NAT
☐ TCPIP
☐ Flood Protection
☐ Access Control
☐ Criptography
☐ Access Profiles
☐ Filtering Rules
File to save report
Browse
Create
Exit

Image 88 – Firewall configuration Report.

This window consists of many distinct options, one for each part of the firewall configuration that may be selected freely. To generate a report, proceed the following way:

1. Check the boxes of corresponding items that should be printed.
2. Click on the “**Browse”** button and choose the HTML page storage directory.
3. Open the directory and select the HTML file to print report.

In case of cancelling the report issue, just click on the “**Cancel”** button**.**

3.16. Entity Search

This option allows locating the entities that contain a determined IP address, interface or service, as well as rules containing a determined entity.

To gain access to the entity location window:

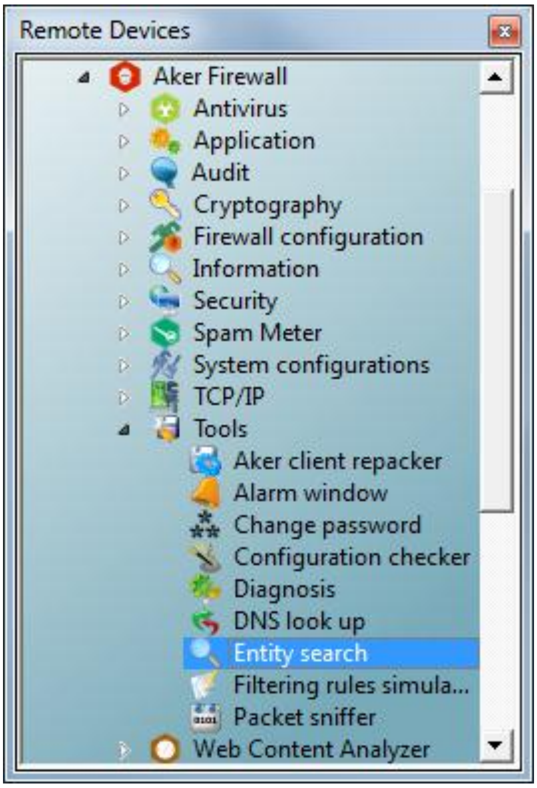

Remote Devices
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simula...
Packet sniffer
Web Content Analyzer

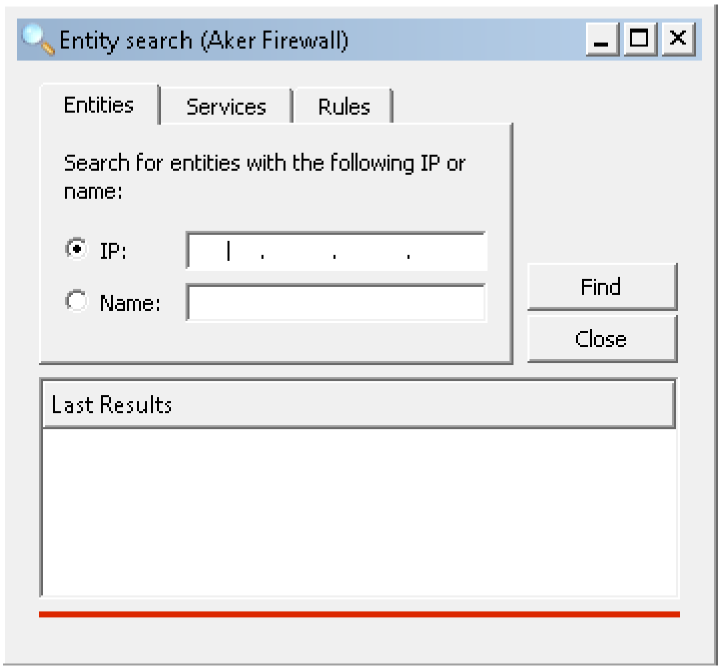
Image 89 – Entity Search access window.

- Click on the firewall administration window > *Tools* menu
- Select *Entity search.*

Entity location window

This window consists of three tabs, each one of them is responsible for a different type of search:

Entities Tab


Entity search (Aker Firewall)
Entities
Services
Rules
Find
Close
Last Results

Search for entities with the following IP or name:

● IP: | . . .

○ Name:

Image 90 – Entity Search (searches for an entity with IP or name and last results).

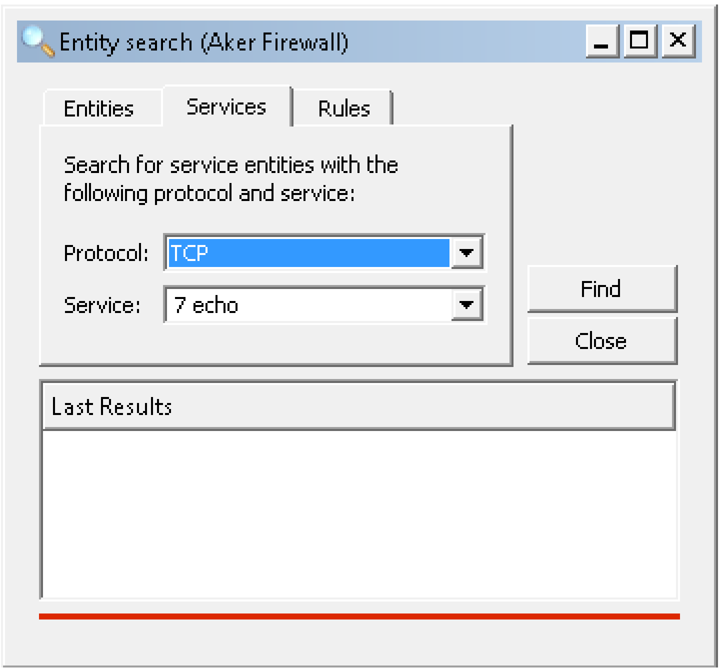
This tab allows the location of entities either by IP address reported or by its name.

Find: start a search from data informed.

Close: closes the entity location window.

By double-clicking upon an entity name or rule, displayed as a search result, the corresponding edition window will open, allowing values to be quickly edited.

Service Tab


Entity search (Aker Firewall)
Entities
Services
Rules
Find
Close
Last Results

Search for service entities with the following protocol and service:

Protocol: TCP

Service: 7 echo

Image 91 – Entity Search (Services, protocol and last results).

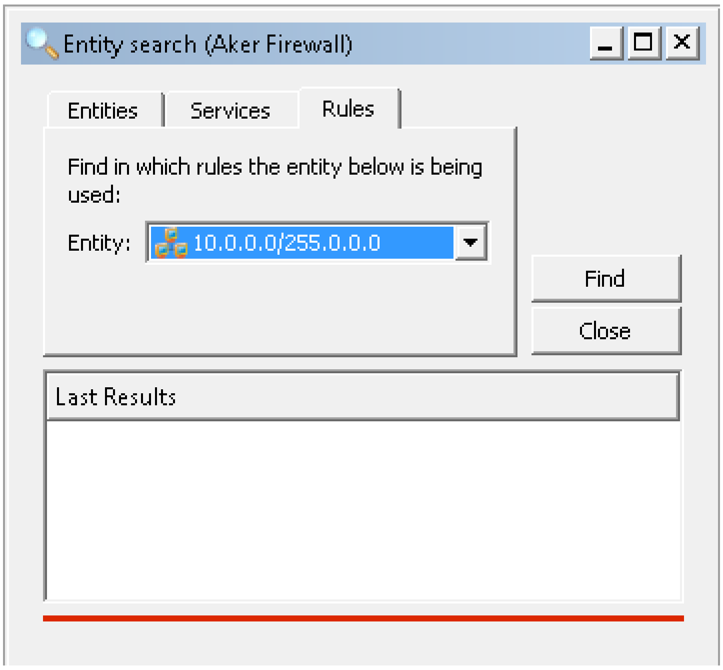
This tab allows *service* type entities containing the specified protocol and service to be located.

Find: begins search from data informed.

Close: closes the entity location window.

By double-clicking upon an entity name or rule, displayed as a search result, the corresponding edition window will open, allowing values to be quickly edited.

Tab Rules



Find in which rules the entity below is being used:

Entity: 10.0.0.0/255.0.0.0

Image 92 – Entity Search (Rules, entities and last results).

This tab allows the location of the rule that the entity belongs to.

Find: This field begins search from the data informed.
Close: This field closes the entity location window.

This tab will only load entities of the following types: Computer, Network, Set and Service.

Entity: When selecting an entity a search is performed delivering the rule number which the entity belongs to. The rules may be **VPN Rules, NAT Rules, Filtering Rules or Filtering Rules within Profiles**, if the entity in question is a Network or a Computer type, a search is conducted to determine if it is present in a Set entity. In case it is, the rules containing this Set entity and its related types will be displayed and printed in the search result, **and as a consequence the rules containing these sets will also be displayed**.

By double clicking upon an entity or rule, displayed as a search result (Set Entities, Filtering Rules, NAT Rules, VPN Rules and Profile), the corresponding edition window will open allowing its values to be quickly edited.

3.17. Alarm Window

This option allows viewing the alarms generated by the firewall, when this option is checked on the Filtering Rules or Action Window.

To gain access to the alarm window, follow the steps below:

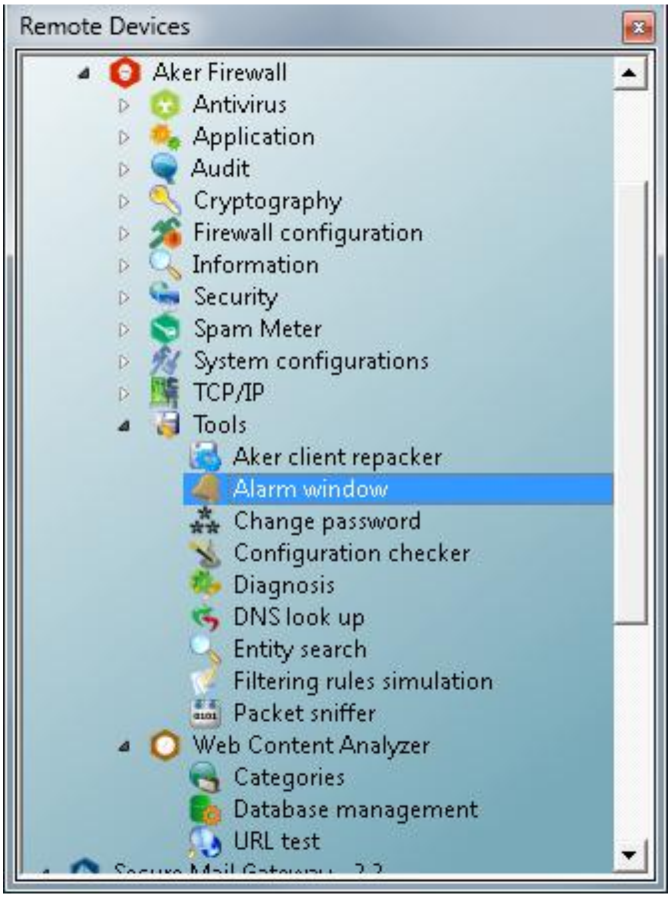

Remote Devices
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer
Web Content Analyzer
Categories
Database management
URL test

Image 93 – Window access to Alarm window.

- Click on the *Tools menu.*
- Select *Alarm window.*

Alarm window

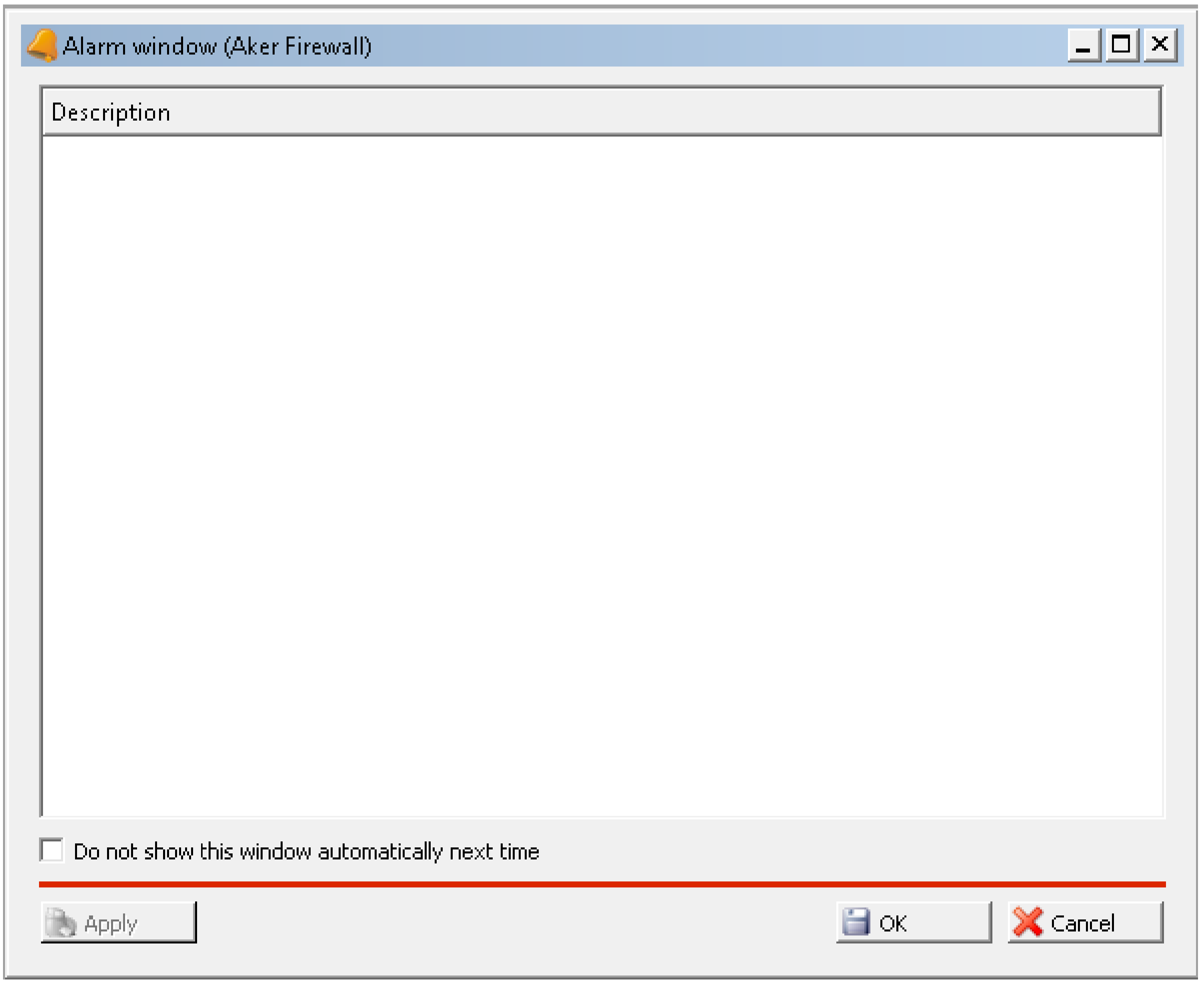

Alarm window (Aker Firewall)
Description
☐ Do not show this window automatically next time
Apply
OK
Cancel

Image 94 – Alarm Window (Description)

This window consists of a description field with the corresponding entries to the action executed by filtering rules.

- The **Close** button closes the window.
- The **Do not show this window automatically next time** box, when checked, will disable the window to open automatically when an event occurs.
- The **Save** button registers the entries on a text log file.
- The **Erase** button deletes all entries displayed on the window.

3.18. Network View

The firewall features a practical system to view the network where it is inserted in a graphic way. To gain access to the *network view* window follow the steps below:

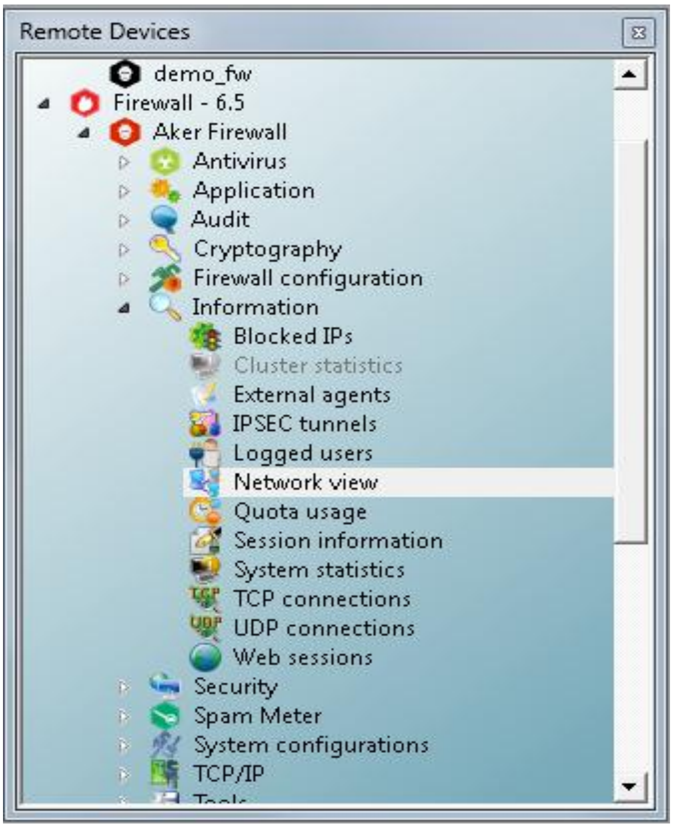

Remote Devices
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP

Image 95 – Access window: Network view.

- Click the “**Information”** menu.
- Select **“Network view”**.

The following window will be displayed:

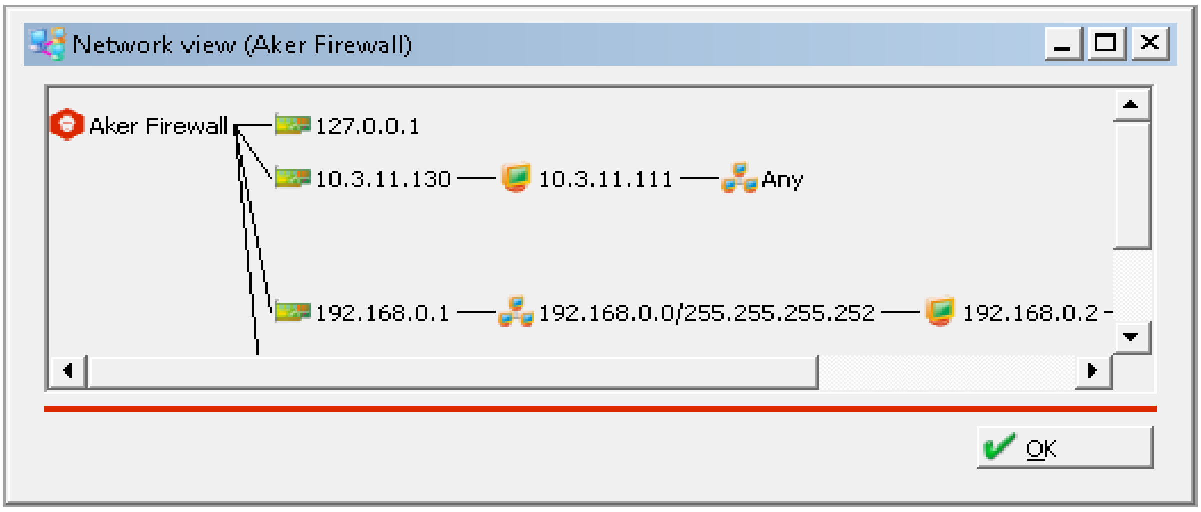

Network view (Aker Firewall)
Aker Firewall
127.0.0.1
10.3.11.130
10.3.11.111
Any
192.168.0.1
192.168.0.0/255.255.255.252
192.168.0.2
OK

Image 96 – Network view

The first item represents the firewall connected to its network interfaces. Each interface is connected to one or more networks or routers that connect to more distant networks. By right-clicking on a network, a menu listing the entities that compose it will appear, enabling the user to edit them.

3.19. System statistics

The System statistics window contains information on the processor usage and system memory usage.

To gain access to this window:

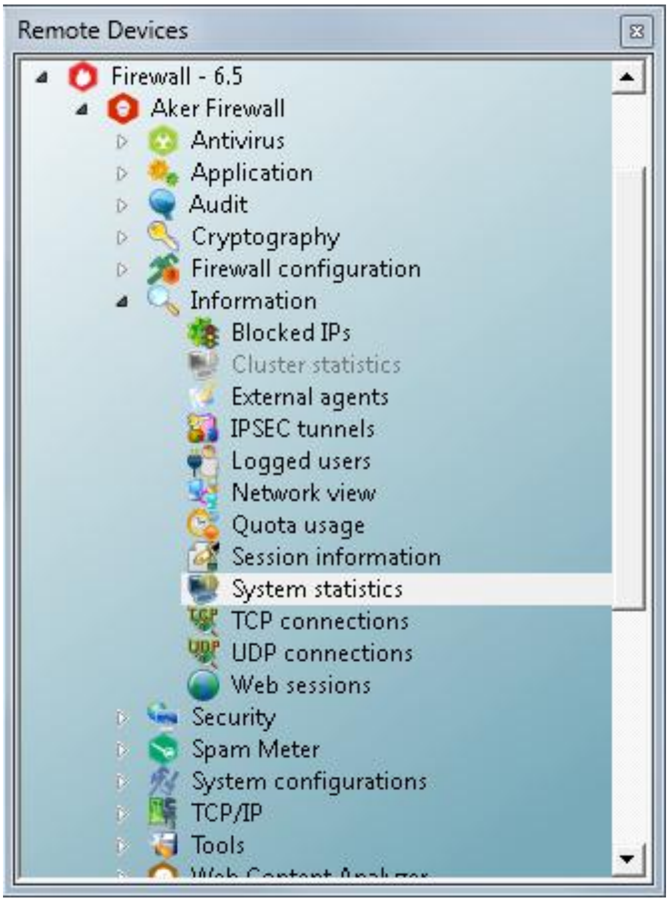
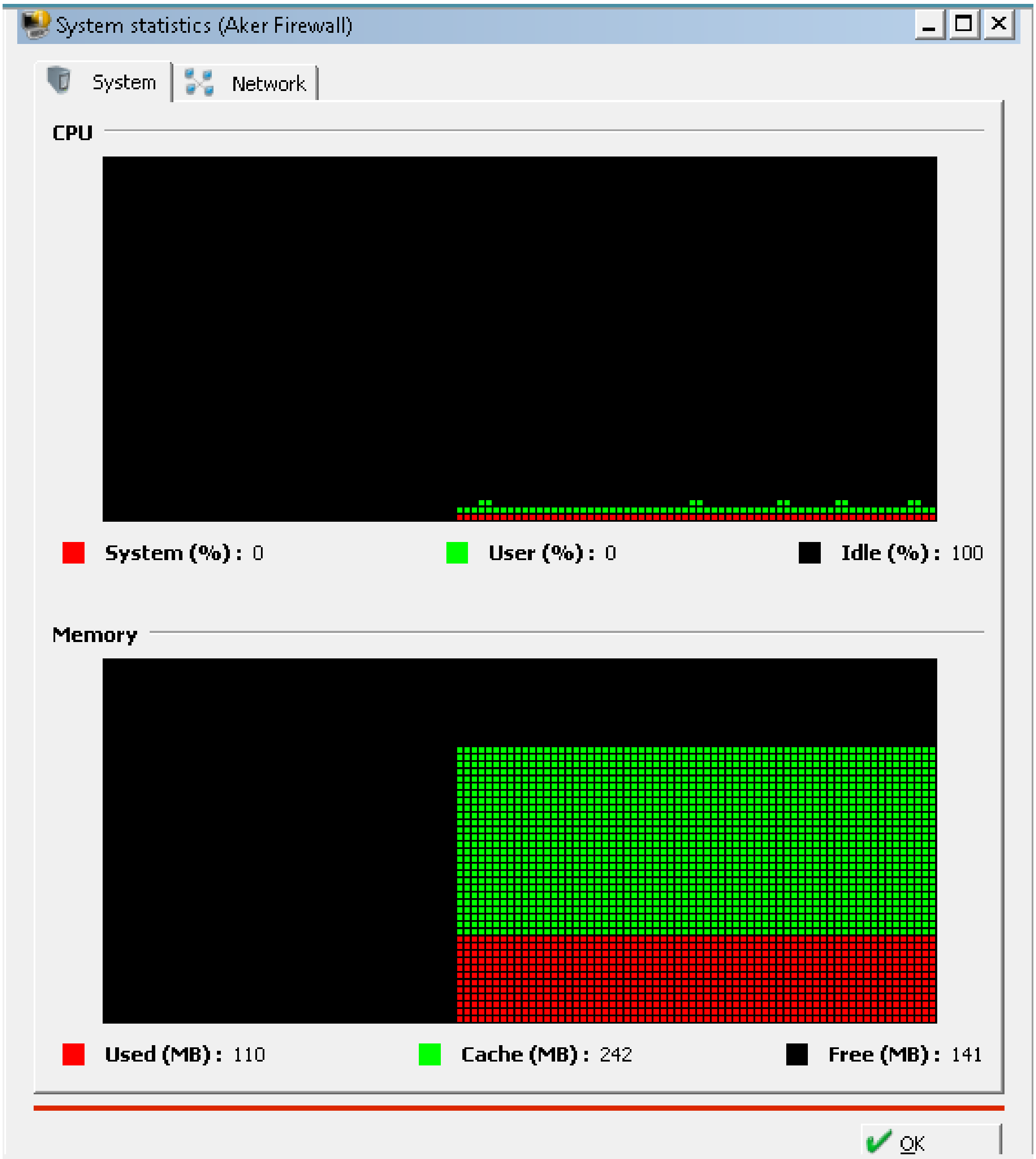

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 97 – Access window: System Statistics.

- Click the firewall administration *Information* menu.
- Select the **“System statistics”** item.

The following window will be displayed:


System statistics (Aker Firewall)
System
Network
CPU
Memory
OK

🟥 System (%) : 0 🟩 User (%) : 0 ⬛ Idle (%) : 100

🟥 Used (MB) : 110 🟩 Cache (MB) : 242 ⬛ Free (MB) : 141

Image 98 – System statistics

At the top of the window, CPU usage information is displayed. This information is divided into three parts: *idle percentage, percentage dedicated to the system and percentage being used by programs* started by the user. At the bottom of the window the system memory status is displayed in Megabytes. This is also divided into three *parts: amount of free memory, amount of memory being used and amount of memory storing cache information.*

Memory amount does not affect the firewall performance significantly. However, a drop in performance may occur if the system has an area of memory swap and is making good use of it, which will only affect proxies.

It is important to note the cache memory is not considered used memory. It is only accessed when the system needs to reopen a program. In case this program is still in cache, reopening will be quicker. However, if the system needs a greater amount of free memory, the area used for cache will be released.

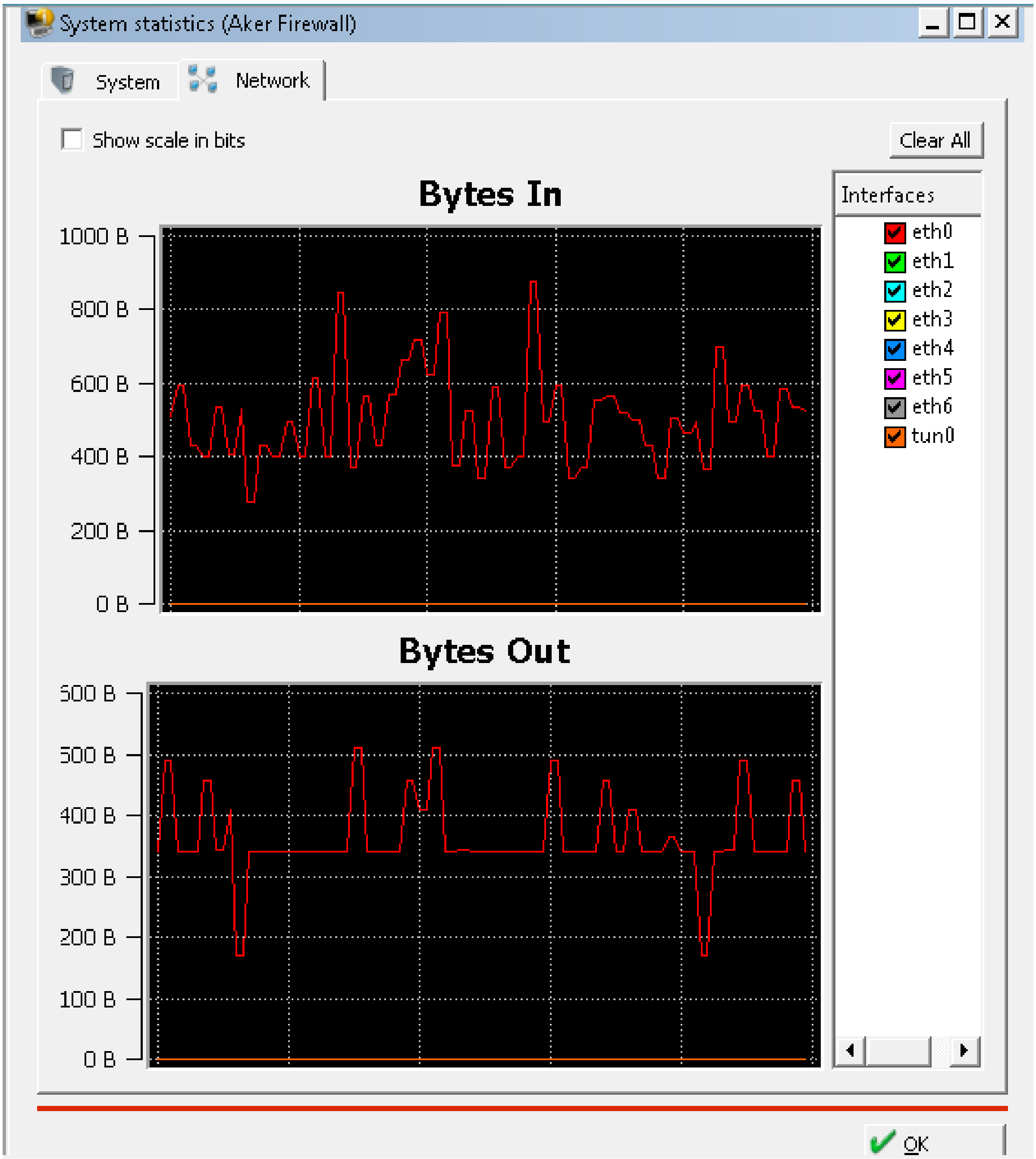

System statistics (Aker Firewall)
System
Network
☐ Show scale in bits
Clear All
Bytes In
1000 B
800 B
600 B
400 B
200 B
0 B
Bytes Out
600 B
500 B
400 B
300 B
200 B
100 B
0 B
Interfaces
☑ eth0
☑ eth1
☑ eth2
☑ eth3
☑ eth4
☑ eth5
☑ eth6
☑ tun0
OK

Image 99 – System statistics report

3.20. Using the Packet Sniffer window

Aker Firewall Sniffer window allows the administrator to capture packets from one or more connections traveling within the firewall. The great advantage of this Sniffer compared to a traditional one is that it is possible to capture packets from several different points within an interface: it is possible to view the packets as they are received (i.e., ciphered and with converted addresses) or exactly before or after filtering, which displays them clearly and with real addresses.

It is important to note the fwpacket command just captures data from the header IP.

Recently the firewall packet sniffer just captures data from the header IP. A request to implement capturing layer 2 information functionalities features has been issued.

To gain access to the Sniffer window:

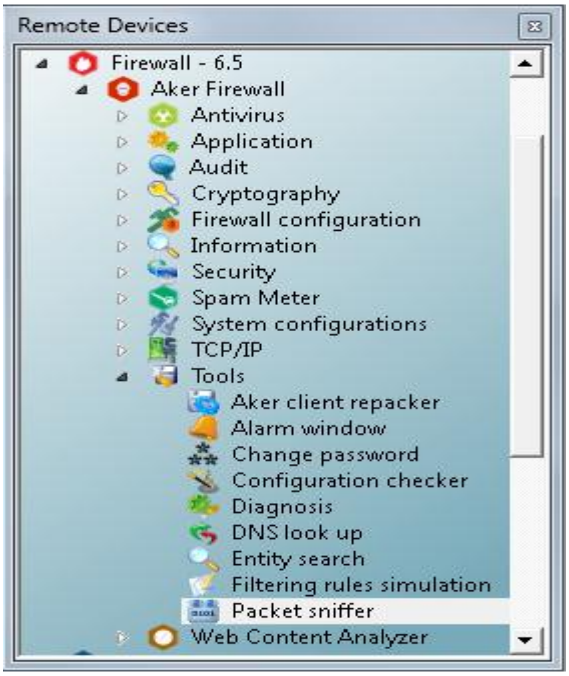

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer
Web Content Analyzer

Image 100 – Window access: Packet Sniffer.

- Click the firewall administration window *Tools* menu.
- Select the **Packet Sniffer** item.

Packet Sniffer window

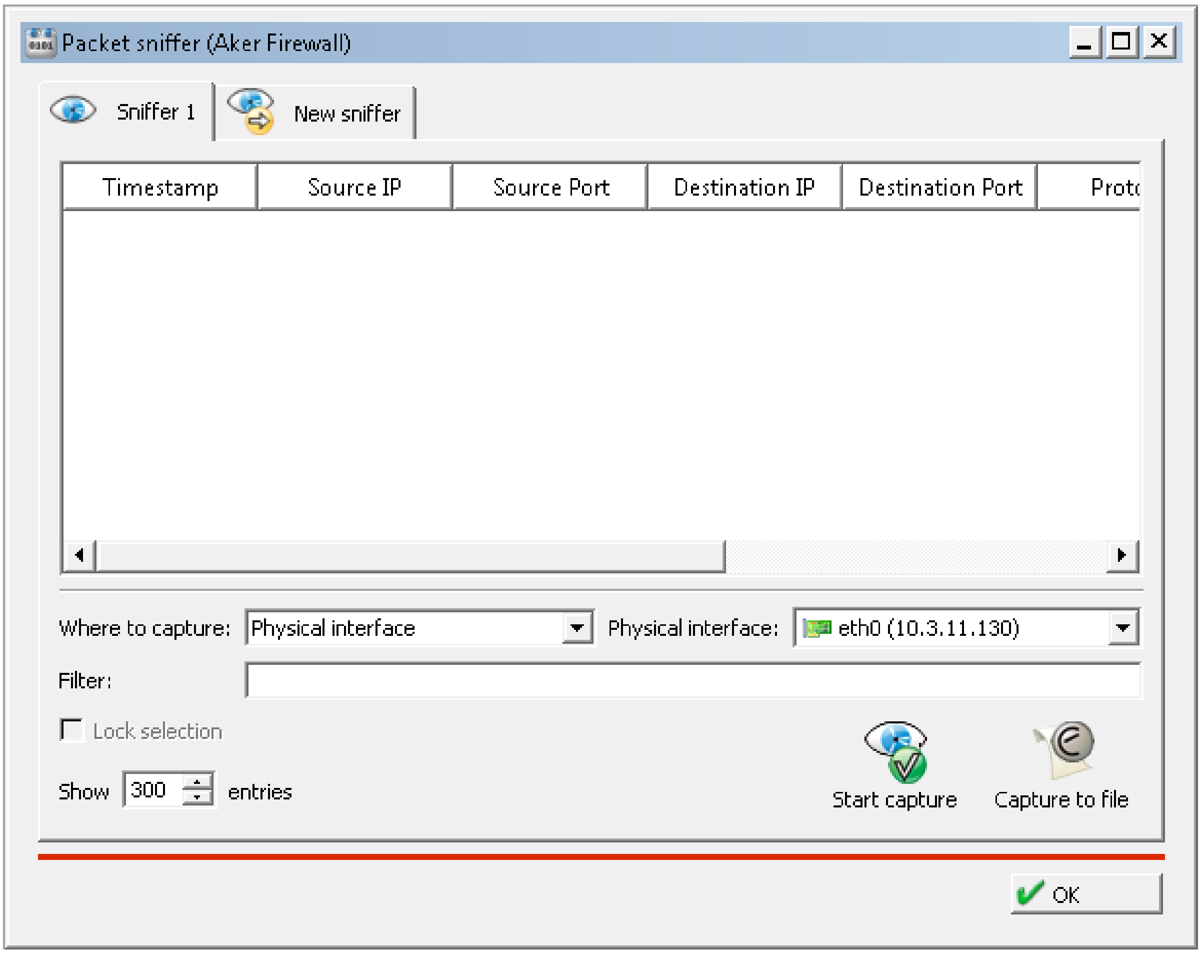

Packet sniffer (Aker Firewall)
Sniffer 1
New sniffer
Timestamp
Source IP
Source Port
Destination IP
Destination Port
Proto
Where to capture:
Physical interface
Physical interface:
eth0 (10.3.11.130)
Filter:
☐ Lock selection
Show 300 entries
Start capture
Capture to file
OK

Image 101 – Packet Sniffer (Sniffer 1)

This window consists of many tabs. Each tab allows traffic capturing in a specific interface or in different points of the same interface. To create new sniffer tabs, click the last tab where the text **New Sniffer** is displayed.

To begin the capture, fill in the following fields:

Where to capture: Defines the spot where captures should take place. The following options are available:

Physical Interface: Defines the capture to take place exactly as packets are received by the firewall.

Before filtering: Defines that the packets should be captured immediately before being filtered, i.e., after being decrypted and having their addresses converted, if that is the case.

After filtering: Defines that the captures will take place only when packets are filtered and viewed decrypted with their addresses converted, if that is the case.

Physical Interface: Defines which interface will be used to capture packets.

Filter: This field defines the filter that will be used in the capture of packets. The purpose of this filter is to limit packets received down to what matters. In case it is left in blank, all packets will be captured. The filter syntax is the same one used in the popular program *tcpdump* and all its options are supported. A summary of the main options that may be used on filters is presented below:

- **dir**

  Indicates the direction on which transfer will take place, to and/or from the identifier.
  Possible directions are src, dst, src or dst e src and dst.
  E.g.:
  ``src foo"
  ``dst net 128.3"
  "src or dst port ftp-data"

- **proto**

  Qualifier restricted to stipulating one kind of protocol. Existent protocol options are ether, ip, arp, rarp, tcp and udp.
  E.g.
  ``ether src foo"
  ``arp net 128.3"
  ``tcp port 21"
  When not stipulated, all existent protocols in option will be undertaken.

- **port**

  Capture packets with the source port or destination. All port expressions may be preceded by tcp or udp, as the example below:
  tcp src port
  Only capture tcp packets with source port.

When the **Lock selection** button is selected, the packet selected will remain always visible on the capture window.

The **Start capture** begins packet capturing, however, results will only be sent to that window.

The **Capture to file** button starts packet captures and records the data on the file specified. This file may be opened after by most traditional Sniffers available in the market.

The **OK** button ends capture and closes the window. In case captures were made for a file, they will be available.

3.21. Viewing the State of External Agents

The State of External Agents window is purely informative and is used to indicate the administrator the state of External Agents. This is very useful when configuring a new external agent or to detect the occurrence of possible problems.

To gain access to External Agents window:

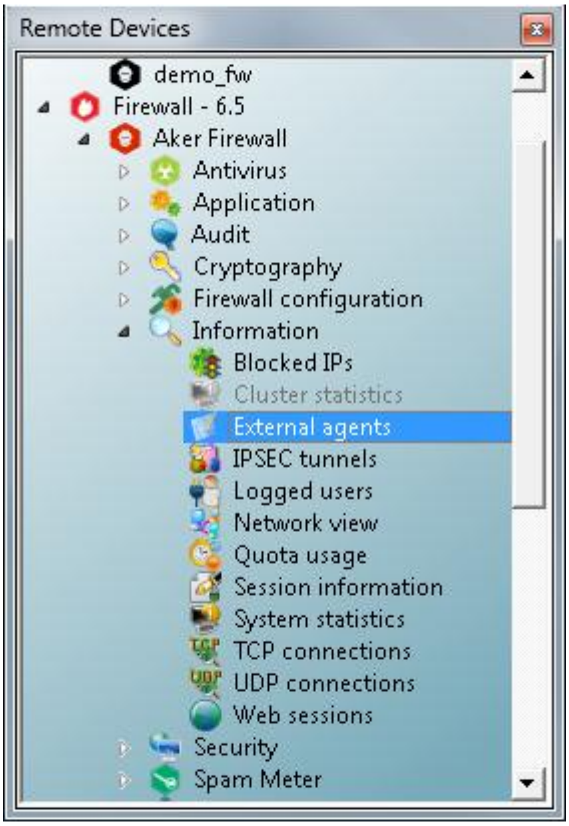
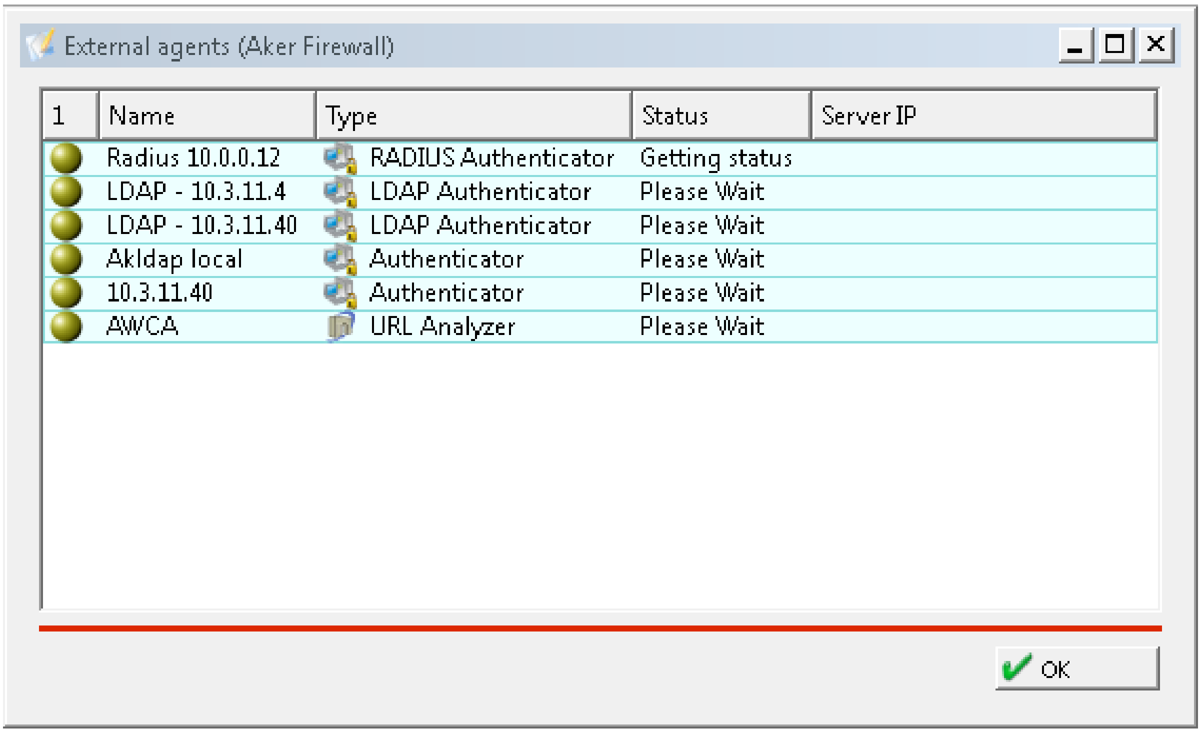

Remote Devices
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter

Image 102 – Access window: External Agents.

- Click the firewall administration window *Information* menu.
- Select *External Agents*.

External Agents window


External agents (Aker Firewall)

1	Name	Type	Status	Server IP
●	Radius 10.0.0.12	RADIUS Authenticator	Getting status	
●	LDAP - 10.3.11.4	LDAP Authenticator	Please Wait	
●	LDAP - 10.3.11.40	LDAP Authenticator	Please Wait	
●	Akldap local	Authenticator	Please Wait	
●	10.3.11.40	Authenticator	Please Wait	
●	AWCA	URL Analyzer	Please Wait	

Image 103 – External Agents (name, type and status).

This window consists of a list naming all active external agents that qualify as one of these following types: **Antivirus Agents, IDS Agents, URL Analyzers, Authenticators** (User/Password, Token, RADIUS e LDAP), **Log Servers and Spam Meter**.

For each agent listed, the following information will be displayed:

Name: External agent entity name.

Type: Type of external agent.

Status: Informs current connection state with external agent. The following states may feature on this column:

- **Indefinite State**: There is not any information available yet regarding this agent state.
- **Connected to main**: Aker Firewall has successfully connected itself to external agent main IP.
- **Connected to first backup**: Aker Firewall has successfully connected itself to the external agent first backup IP. For some reason, initial connection with main IP was not possible.

- **Connected to second backup**: Aker Firewall has successfully connected itself to external agent second backup IP. For some reason, initial connection with first IP was not possible.
- **Connection Error**: Due to a communication problem with the external agent, no connection has been established. Verify events for more information.
- **Internal Error**: Connection with external agent was not possible due to an internal problem. Verify events for more information.
- **Virus not detected**; This state only appears on antivirus agents; it indicates that even though Aker Firewall has managed to properly connect itself to the agent, it was not able to detect the virus test sent by the firewall. Verify antivirus configuration.

Server IP: One or more external agents IP addresses with which the firewall has connected itself.

For log servers, besides **Connected** and **Error** states, there is one more state: **Partially Connected**, this happens when a server is available (first and second backup) however the agent is not connected to all of them.

3.22. Using the Configurations Checker

Configurations Checker is window that will be displayed every time Aker Firewall is started and its initial configuration have not yet been completed. It works to call in a simpler way the assistants that do each one of the product configuration main steps.

It is also possible to call the ***Configuration Checker*** in any moment. To do it, shall follow the steps above:

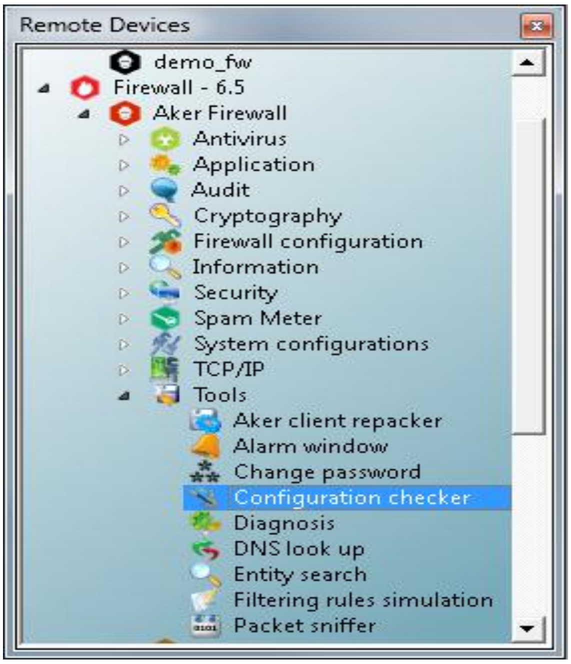
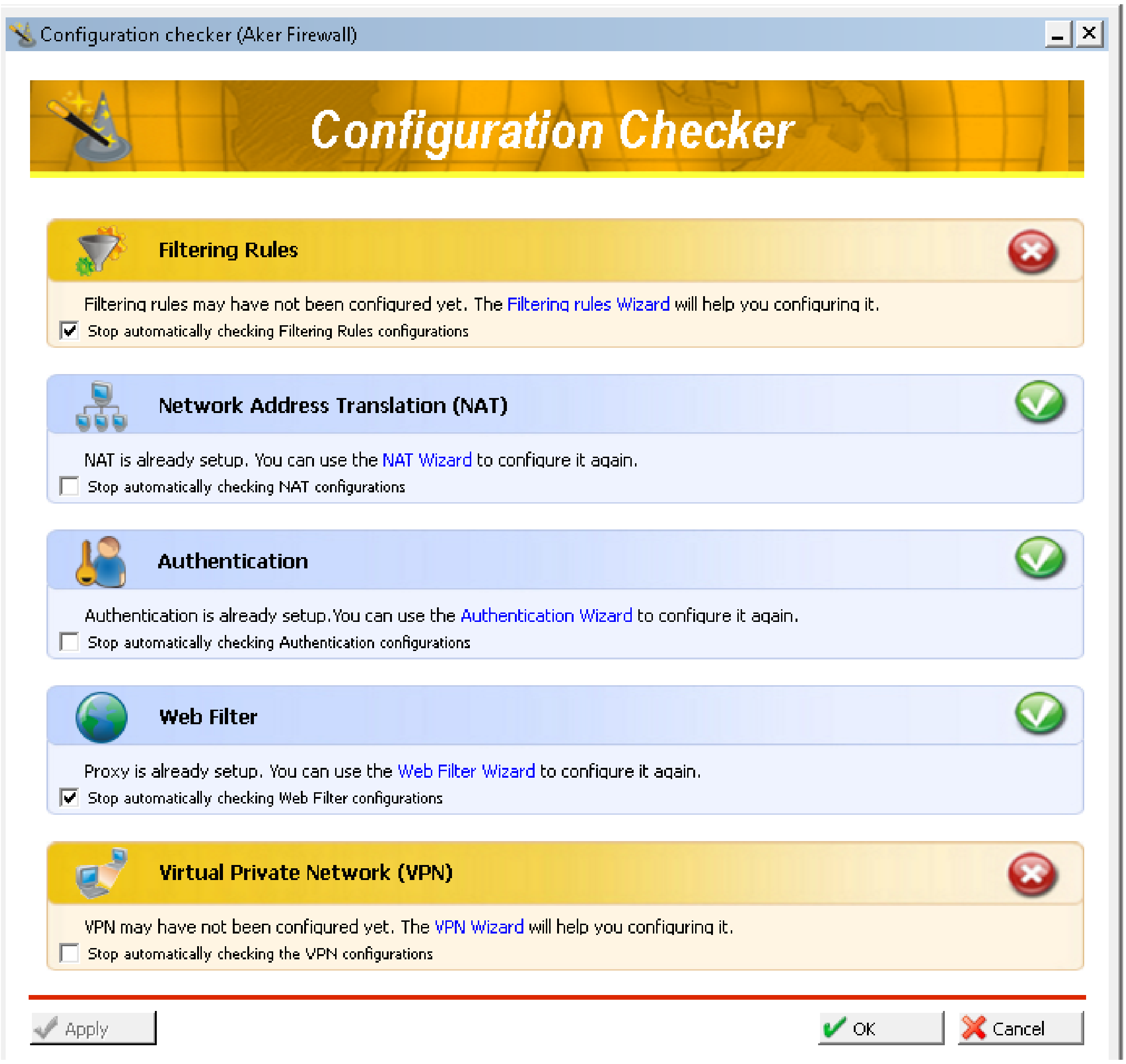

Remote Devices
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer

Image 104 – Access window: Configuration checker

- Click on the firewall administration *Tools* menu.
- Select *Configuration checker*.

Configurations Checker Window



Configuration checker (Aker Firewall)

Configuration Checker

Filtering Rules

Filtering rules may have not been configured yet. The Filtering rules Wizard will help you configuring it.

☑ Stop automatically checking Filtering Rules configurations

Network Address Translation (NAT)

NAT is already setup. You can use the NAT Wizard to configure it again.

☐ Stop automatically checking NAT configurations

Authentication

Authentication is already setup.You can use the Authentication Wizard to configure it again.

☐ Stop automatically checking Authentication configurations

Web Filter

Proxy is already setup. You can use the Web Filter Wizard to configure it again.

☑ Stop automatically checking Web Filter configurations

Virtual Private Network (VPN)

VPN may have not been configured yet. The VPN Wizard will help you configuring it.

☐ Stop automatically checking the VPN configurations

Image 105 – Configurations checker

This window consists of 5 distinct configuration groups. Each configured group is displayed in blue and in Orange in case it has not been configured yet. For each group, it is possible to click the **Wizard** link to rely on the responsible agent implementation for the group configuration. In case of configurations that will never be applied (a firewall that does not perform VPN, for instance), it is possible to disable configuration verification by checking the **Stop automatically checking the VPN configurations** for the desired group.

- The **Apply** button saves verification options and keeps the window open.
- The **OK** button closes the window and saves changes.
- The **Cancel** button closes the window and discards any modifications applied.

It is important to observe that cache memory is not considered used memory. It is only accessed when the system needs to reopen a program. In case this program is still in cache, reopening it takes less time. However, if the system needs a greater amount of free memory, the cache area is released.

It is recommended that the configurations be made in the order which the groups are presented, from top to bottom.

3.23. Diagnosis

Aker Firewall performs basic connectivity tests:

- Ping in default route;
- Ping in unknown places (i.e. Google DNS);
- DNS Tests;
- HTTP Test;
- Traceroute command;
- Netstat command;
- Nslookup command. know

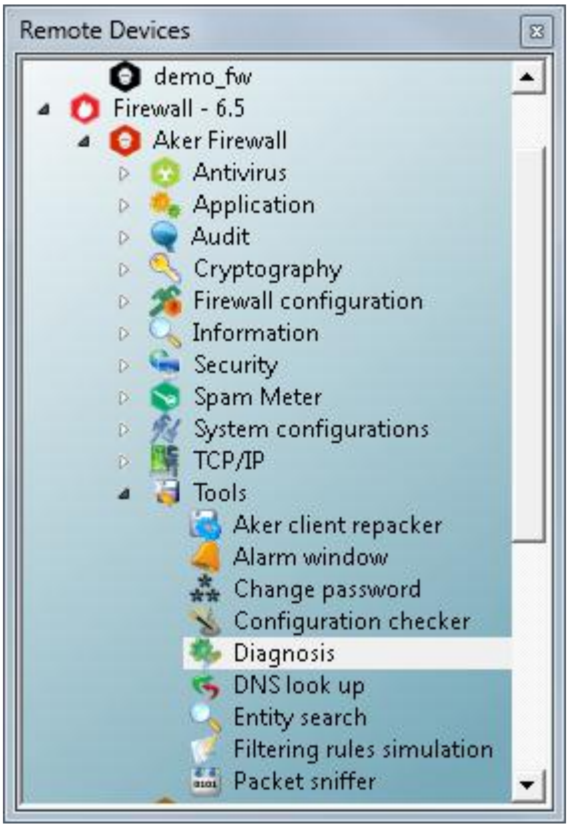
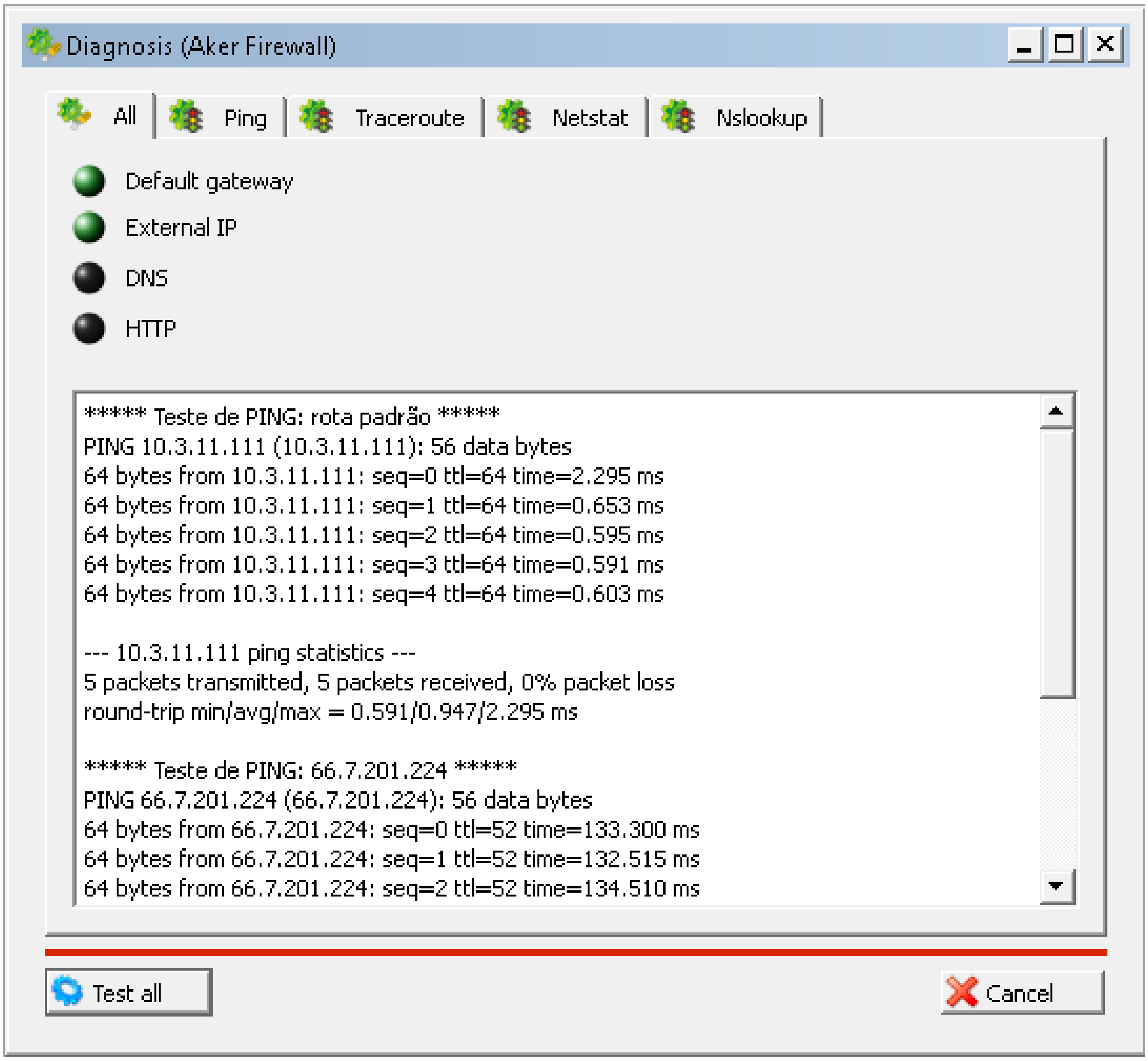

Remote Devices
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Aker client repacker
Alarm window
Change password
Configuration checker
Diagnosis
DNS look up
Entity search
Filtering rules simulation
Packet sniffer

Image 106 – Access Window: Diagnosis.

Presented below are the screens for each tab.

All tabs

Internet access status is returned to user.


Diagnosis (Aker Firewall)
All
Ping
Traceroute
Netstat
Nslookup
Default gateway
External IP
DNS
HTTP
Test all
Cancel

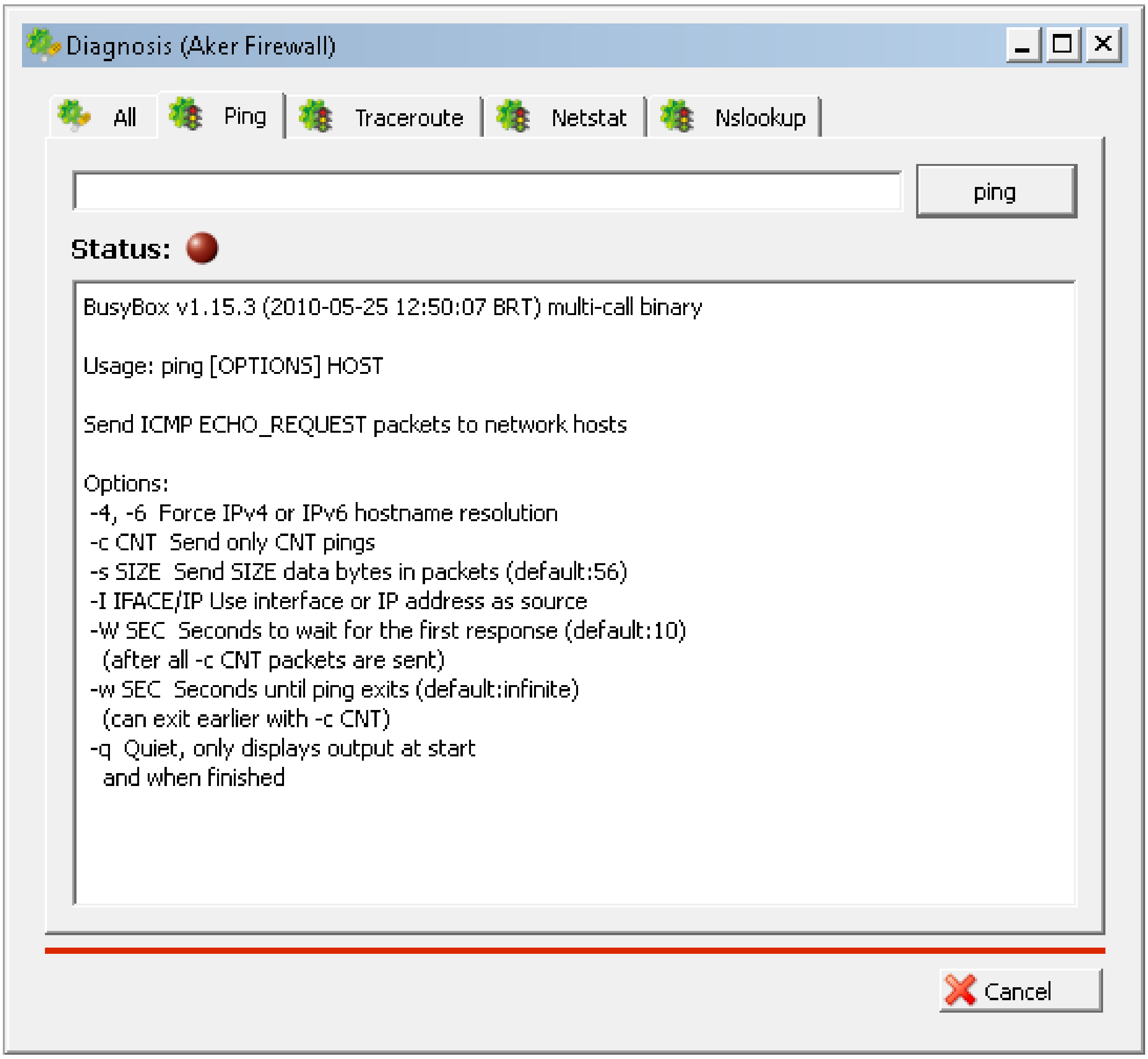
```
***** Teste de PING: rota padrão *****
PING 10.3.11.111 (10.3.11.111): 56 data bytes
64 bytes from 10.3.11.111: seq=0 ttl=64 time=2.295 ms
64 bytes from 10.3.11.111: seq=1 ttl=64 time=0.653 ms
64 bytes from 10.3.11.111: seq=2 ttl=64 time=0.595 ms
64 bytes from 10.3.11.111: seq=3 ttl=64 time=0.591 ms
64 bytes from 10.3.11.111: seq=4 ttl=64 time=0.603 ms

--- 10.3.11.111 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.591/0.947/2.295 ms

***** Teste de PING: 66.7.201.224 *****
PING 66.7.201.224 (66.7.201.224): 56 data bytes
64 bytes from 66.7.201.224: seq=0 ttl=52 time=133.300 ms
64 bytes from 66.7.201.224: seq=1 ttl=52 time=132.515 ms
64 bytes from 66.7.201.224: seq=2 ttl=52 time=134.510 ms
```

Image 107 –Diagnosis Window: All

To gain access, just click the **“Test All”** button and the data will be displayed.

Ping Tab

Ping Tab performs an ICMP (ping) test the IP address or the DNS name typed in. This test validates Aker Firewall connectivity with the tested address.



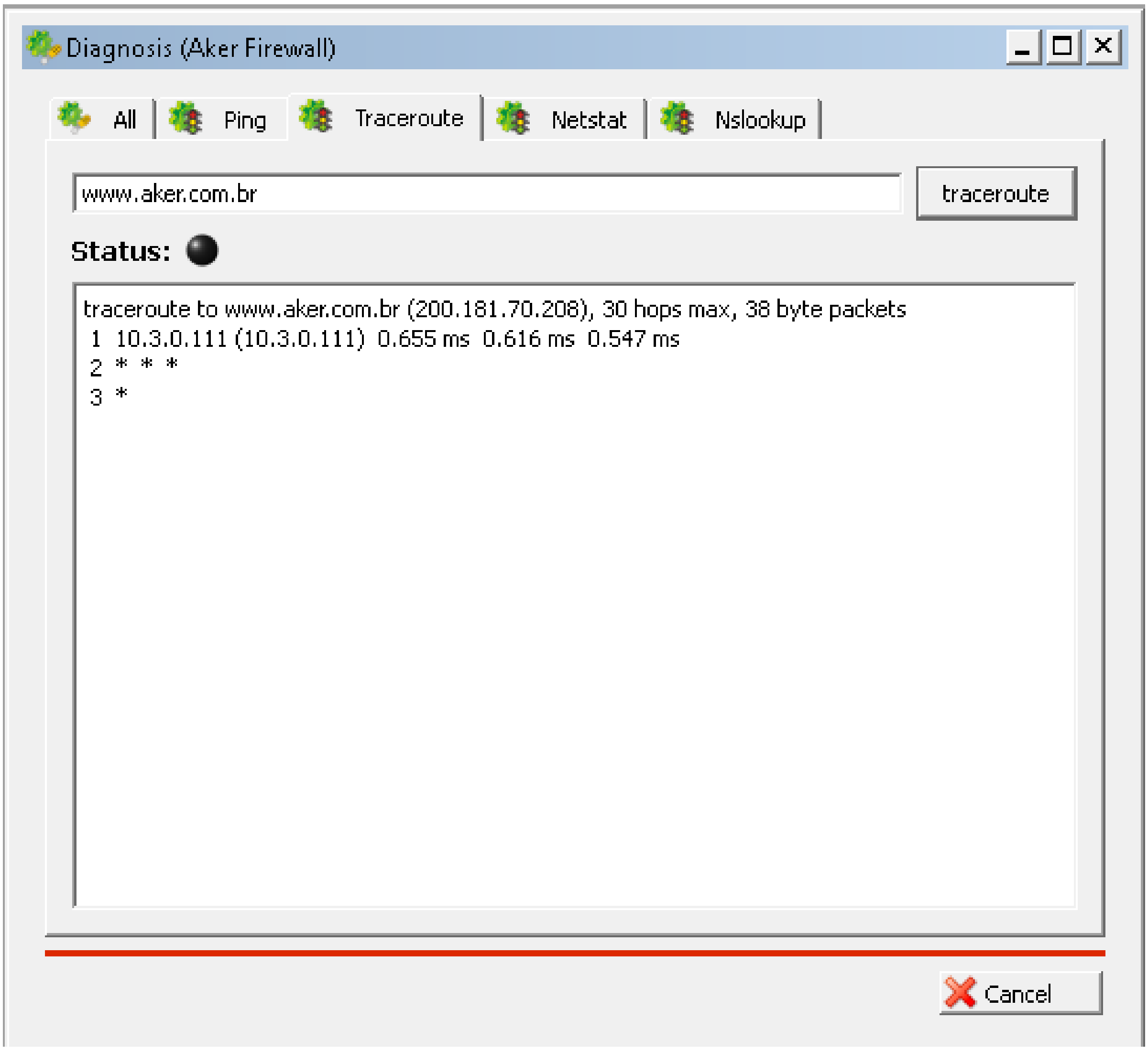
```
BusyBox v1.15.3 (2010-05-25 12:50:07 BRT) multi-call binary

Usage: ping [OPTIONS] HOST

Send ICMP ECHO_REQUEST packets to network hosts

Options:
 -4, -6  Force IPv4 or IPv6 hostname resolution
 -c CNT  Send only CNT pings
 -s SIZE  Send SIZE data bytes in packets (default:56)
 -I IFACE/IP Use interface or IP address as source
 -W SEC  Seconds to wait for the first response (default:10)
   (after all -c CNT packets are sent)
 -w SEC  Seconds until ping exits (default:infinite)
   (can exit earlier with -c CNT)
 -q  Quiet, only displays output at start
   and when finished
```

Image 108 – Diagnosis Window: Ping

To gain access, just type in the chosen IP address and click the **“ping”** button and the data is then displayed.

Traceroute Tab

Traceroute performs a trace between Aker Firewall and the IP address or name typed in.


Diagnosis (Aker Firewall)
All
Ping
Traceroute
Netstat
Nslookup
traceroute
Status:
Cancel

www.aker.com.br

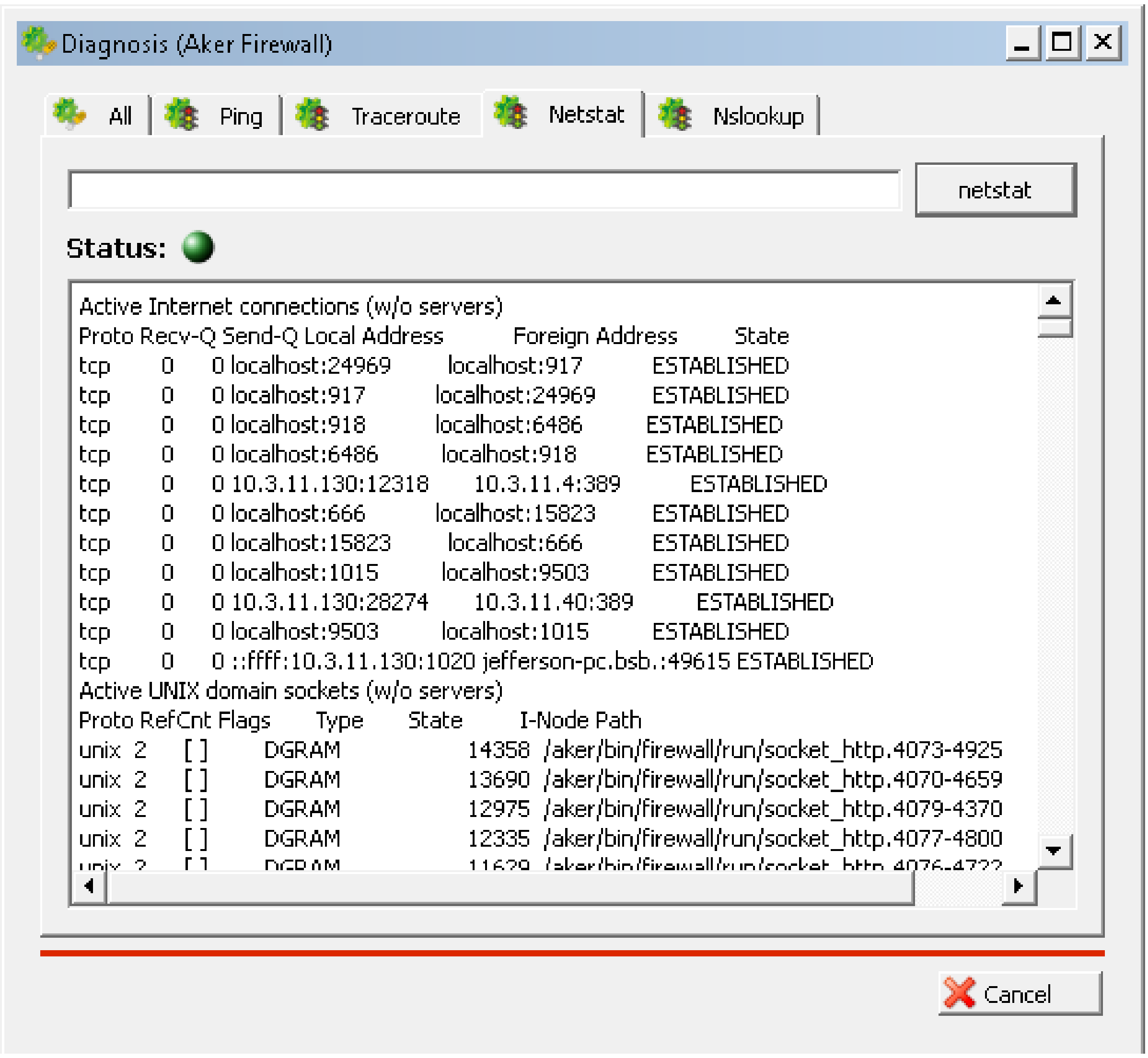
```
traceroute to www.aker.com.br (200.181.70.208), 30 hops max, 38 byte packets
 1  10.3.0.111 (10.3.0.111)  0.655 ms  0.616 ms  0.547 ms
 2  * * *
 3  *
```

Image 109 – Diagnosis Window: Traceroute.

To gain access, just type in the IP address or name and click the **“Traceroute”** button and the data is then displayed.

Netstat Tab

Netstat tab returns the status of all connections belonging to Aker Firewall.



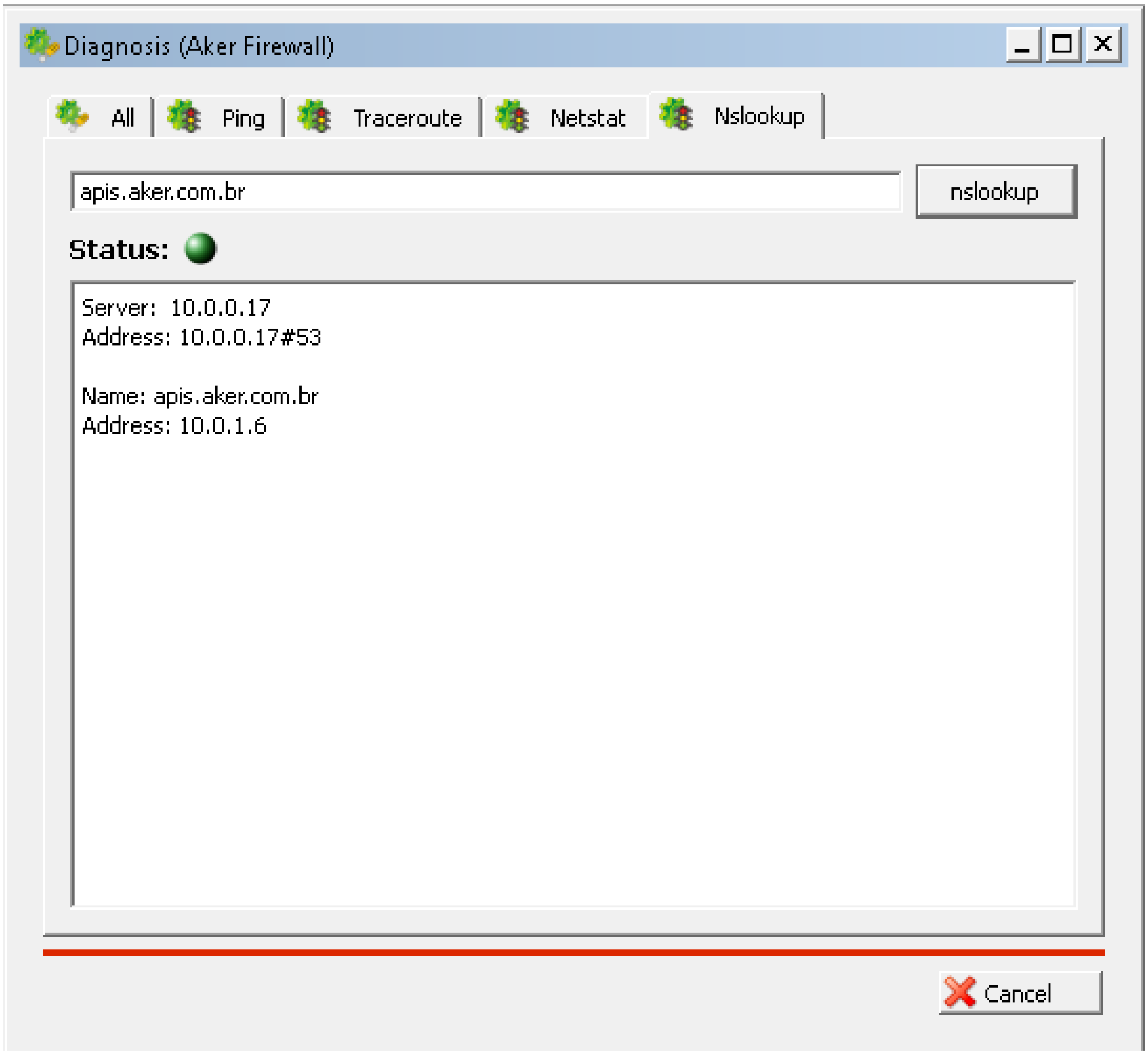
```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 localhost:24969         localhost:917          ESTABLISHED
tcp        0      0 localhost:917           localhost:24969        ESTABLISHED
tcp        0      0 localhost:918           localhost:6486         ESTABLISHED
tcp        0      0 localhost:6486          localhost:918          ESTABLISHED
tcp        0      0 10.3.11.130:12318       10.3.11.4:389          ESTABLISHED
tcp        0      0 localhost:666           localhost:15823        ESTABLISHED
tcp        0      0 localhost:15823         localhost:666          ESTABLISHED
tcp        0      0 localhost:1015          localhost:9503         ESTABLISHED
tcp        0      0 10.3.11.130:28274       10.3.11.40:389         ESTABLISHED
tcp        0      0 localhost:9503          localhost:1015         ESTABLISHED
tcp        0      0 ::ffff:10.3.11.130:1020 jefferson-pc.bsb.:49615 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ]         DGRAM                    14358  /aker/bin/firewall/run/socket_http.4073-4925
unix  2      [ ]         DGRAM                    13690  /aker/bin/firewall/run/socket_http.4070-4659
unix  2      [ ]         DGRAM                    12975  /aker/bin/firewall/run/socket_http.4079-4370
unix  2      [ ]         DGRAM                    12335  /aker/bin/firewall/run/socket_http.4077-4800
```

Image 110 – Diagnosis Window (Netstat tab)

Just click the **"Netstat"** button and data will be displayed on the screen.

Nslookup Tab

The *Nslookup* tab performs the resolution of the names typed for their respective IP addresses, this test is important to validate AKER Firewall DNS configuration.


Diagnosis (Aker Firewall)
All
Ping
Traceroute
Netstat
Nslookup
nslookup
Status:
Cancel

apis.aker.com.br

```
Server:  10.0.0.17
Address: 10.0.0.17#53

Name: apis.aker.com.br
Address: 10.0.1.6
```

Image 111 – Diagnosis Window (Nslookup tab)

To gain access, just type in the server name to its respective IP address and then click the **“*Nslookup*”** button, data is then displayed on the screen.

Administering Firewall users

4. Administering Firewall users

This chapter shows how to create users to manage Aker Firewall remotely.

What are Aker Firewall users?

In order to Aker Firewall be remotely managed, administrators need to be recognized and validated by the system. This validation is done through passwords, therefore, to make it possible; each administrator should be previously registered with login as well as password.

Beside this, Aker Firewall allows the existence of many distinct administrators, each one being responsible for a specific administration task. Besides making the management easier, it also allows greater control and greater security. It is user registration that defines the respective attributions of each administrator.

4.1. Administrator Users

To gain access to the Administrative Users Window via remote interface, follow the steps below:

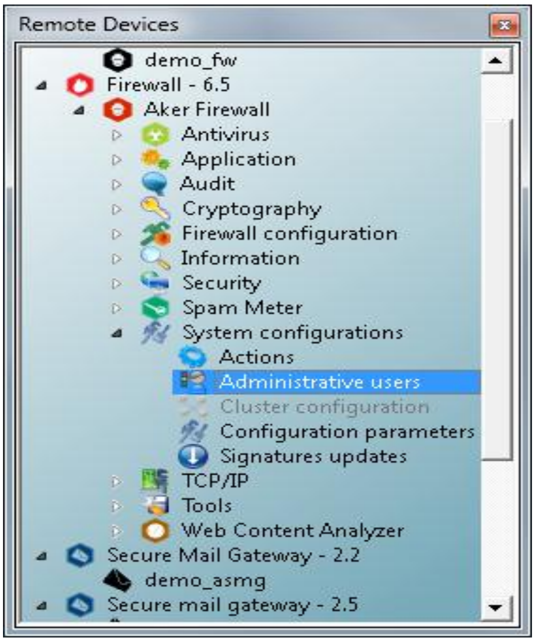

Remote Devices
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
Actions
Administrative users
Cluster configuration
Configuration parameters
Signatures updates
TCP/IP
Tools
Web Content Analyzer
Secure Mail Gateway - 2.2
demo_asmg
Secure mail gateway - 2.5

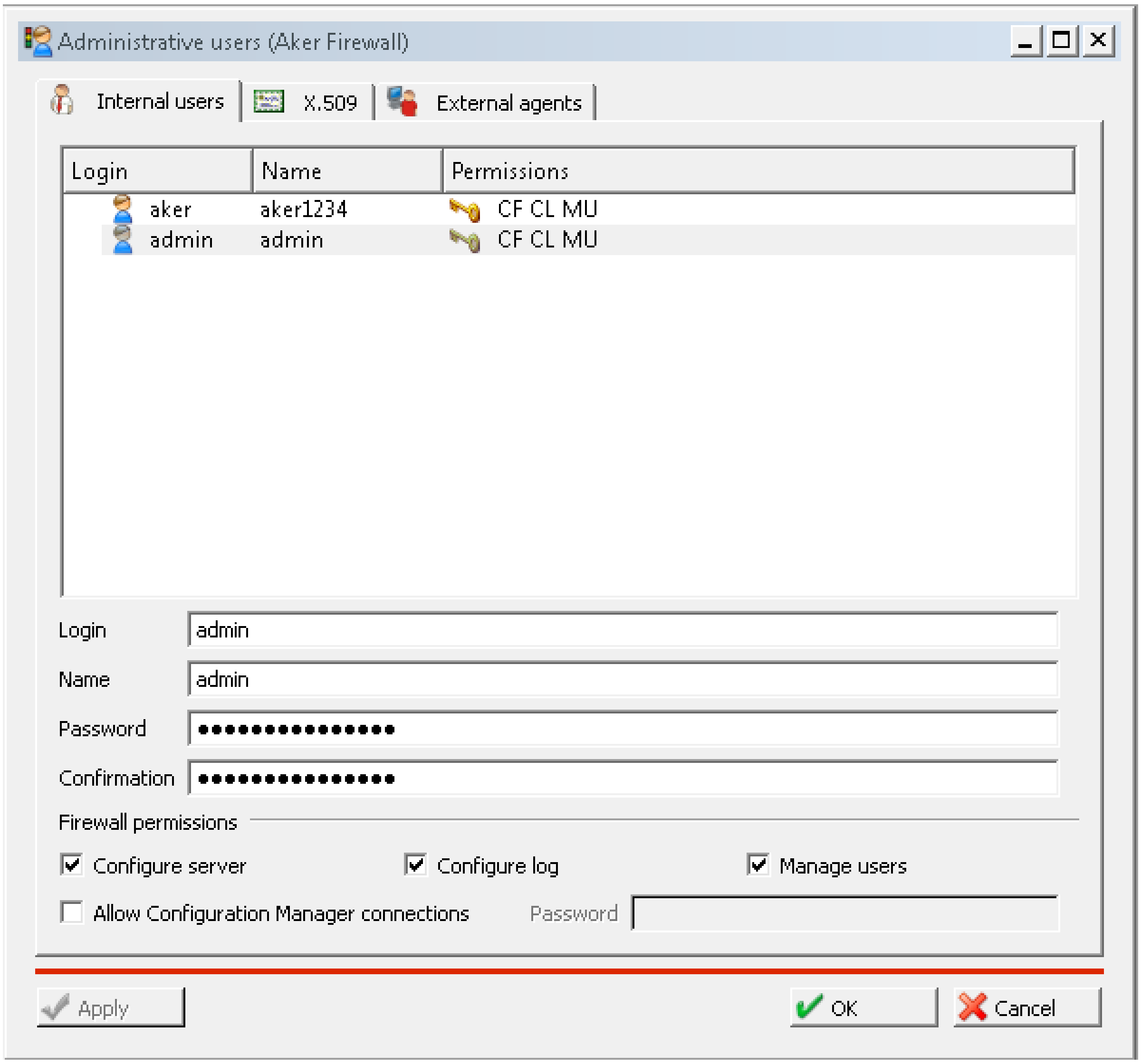
Image 112 – Access to Administrative Users Window

- Click ***System Configuration*** on the firewall window to be administrated.
- Select the ***Administrative Users*** item.

This option is only enabled when the user on the open remote session has been granted authority to manage users. This will be addressed in detail on the next topic.

Administrative Users Window

Internal Users tab


Administrative users (Aker Firewall)
Internal users
X.509
External agents
Firewall permissions
Apply
OK
Cancel

Login	Name	Permissions
aker	aker1234	CF CL MU
admin	admin	CF CL MU

Login: admin
Name: admin
Password: ●●●●●●●●●●●●●●●
Confirmation: ●●●●●●●●●●●●●●●

☑ Configure server ☑ Configure log ☑ Manage users

☐ Allow Configuration Manager connections Password

Image 113 – Administrator Users Window (Internal users).

This window consists of a list of all users currently defined to access the firewall administration, in addition to a shared secret (or password) with centralized administration by Aker Configuration Manager. Without the shared secret, configurations may only be made by registered users.

For each user login, full name, permissions granted will be displayed.

- The **OK** closes the Administrator Users Window and saves all changes.
- The **Apply** button permanently applies the changes made by a determined user without closing the window.
- The **Cancel** button closes the Administrator Users Window and discards any alterations made.
- When a user is selected, his or her complete attributes are displayed in the *Permissions* fields.

To change a user attributes please follow the steps below.

1. Select user to be altered by clicking his or her name. At this moment, attributes are displayed on the fields after user listings.

2. Change the values of all desired attributes and click on the **Apply** or **OK** button. From this moment onwards, changes are effective.

   To include a user to the list, proceed the following way:

1. Right-click anywhere within the reserved space for the list (the **Insert** button shows up) and select the **Include** option from the pop-up menu or click the icon, which represents inclusion on the toolbar.
2. Fill in the fields of users to be included and click the **Apply** or **OK** buttons.

To remove a user from a list, proceed the following way:

1. Select user to be removed, click his or her name and then click the icon , which represents removal on the toolbar, or right-click the name of the user to be removed then select the ***Delete*** option on the pop-up menu.

Meaning of a user attributes

- **Login**

This is user identification for the firewall. There cannot be two users with the same login. This login is requested when the firewall administrator establishes a remote session.

Login should have from 1 e 14 characters. There is no difference between uppercase and lowercase in this field.

- **Name**

This field contains the user associated to the login full name. Its objectives are those of information, not being used for any validation.

This name should have a number of characters in length between 0 e 40.

- **Password**

This field is used in set with the login field to identify users to Aker Firewall. When passwords are typed, asterisks "*" are displayed on the screen, instead of letters themselves.

The password field should contain at most 14 characters. Its minimum size is configured by means of the interface parameters window (for more information see the *Using remote interface* topic). **In this field, uppercase and lowercase are both considered different.**

It is extremely important that passwords be lengthy, the closest possible to the limit of 14 characters. Over and above this the password should contain a combination of uppercase and lowercase, numbers and special characters (special characters are those found on a keyboard that are neither letters nor numbers: "$","&",”]", and so on.). Never use words in any language or just numbers to generate passwords.

- **Confirmation**

This field serves to confirm the password typed in the previous field, once asterisks are displayed on screen, instead of characters themselves.

- **Permissions**

This field defines what a user can do within Aker Firewall. It consists of three options that may be single marked.

The goal of these permissions is to enable the creation of a decentralized administration for the firewall. It is possible, for instance, for a company that has many departments and many firewalls to assign one administrator responsible for configuring each firewall and one central administrator with the task of supervising administration. This supervisor would be the only person capable of deleting and altering log configuration and firewall events. This way, even though each department has autonomy over administration, it is possible to have central control over configurations altered by each administrator, when each alteration was made by and by whom. This is a very important internal auditing resource and increases administration security.

In case a user does not have any authority attributes, then, he is granted the permission to solely visualize the firewall setup and compress log and event files.

- **Firewall setup**

  When this permission is marked, the user in question can manage the firewall, meaning, change entity setup, filtering rules, address translation, encryption, proxies e setup parameters that are not log related.

- **Configure log**

  When this option is marked, the user in question is authorized to change log related parameters (such as log permanence), change the Action Window configuration (for both, messages and parameters) and permanently delete logs and events.

- **Manage Users**

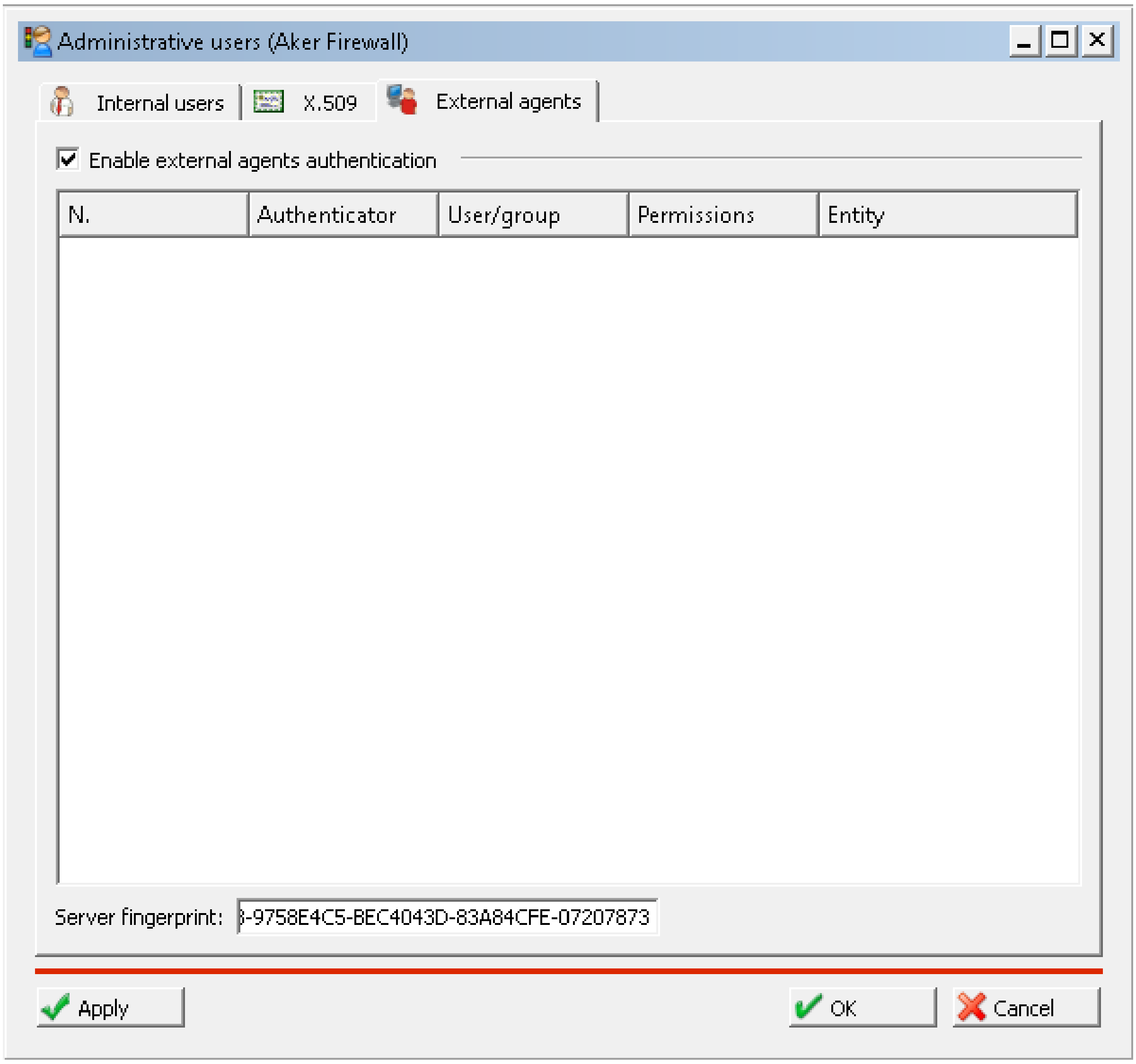
  When this option is marked, the user in question has access to users' administration window, and can add, edit and delete other users.

  A user with this level of authority may only create edit or delete users with equal or smaller authority levels (for instance, if a user has levels to manage other users and configure logs, then he may also create users, without authority, that may only configure logs, that may only create new users or only manage users and configure logs. A user that configures the firewall may never be created, edited or deleted by this level of authority).

- **Allow Configuration Manager connections**

  This option enables/disables access to Aker Firewall via Configuration Manager. As connections are enabled, the common password to firewall and manager (shared secret) should be informed.

External Agents Tab


Administrative users (Aker Firewall)
Internal users
X.509
External agents
N.
Authenticator
User/group
Permissions
Entity
Apply
OK
Cancel

☑ Enable external agents authentication

Server fingerprint: -9758E4C5-BEC4043D-83A84CFE-07207873

Image 114 – Administrator Users: External agents.

This tab consists of configuring external agents that are applied in the authentication of users that administer the firewall, defining, like the access authentication rules.

Enable authentication via external agents

Selecting this option allows user authentication by means of external agents previously registered on the firewall. It also allows external authenticator definition, which user/group it belongs to, its access permissions and the definition of entities the user will use to connect to the firewall.

Authenticator

By right-clicking on the authenticator option, an authenticator (external agent) may be selected and enabled on the *Methods* tab of *Authentication* window. This authenticator is responsible for mediating the interface authentication process with the firewall.

User/Group

Users and groups are related to the chosen authenticator. A single user or a group of users may be associated.

Permissions

This field defines what a user can do within Aker Firewall. It consists of three options that may be single checked.

The goal of these permissions is to make possible the creation of a decentralized administration for the firewall. It is possible, for instance, in a company which has many departments and many firewalls, set an administrator responsible for the setup of each firewall, and one main administrator responsible with the task of supervise and manage. This supervisor would be the only person capable of deleting and changing a ***configure log and firewall events.*** This way, despite each department has certain autonomy of administration, it is possible to have a Central Control that records each administrator change in the setup, and when he made the change. This is a very important resource to conducts internal audits, beside increase the security of administration.

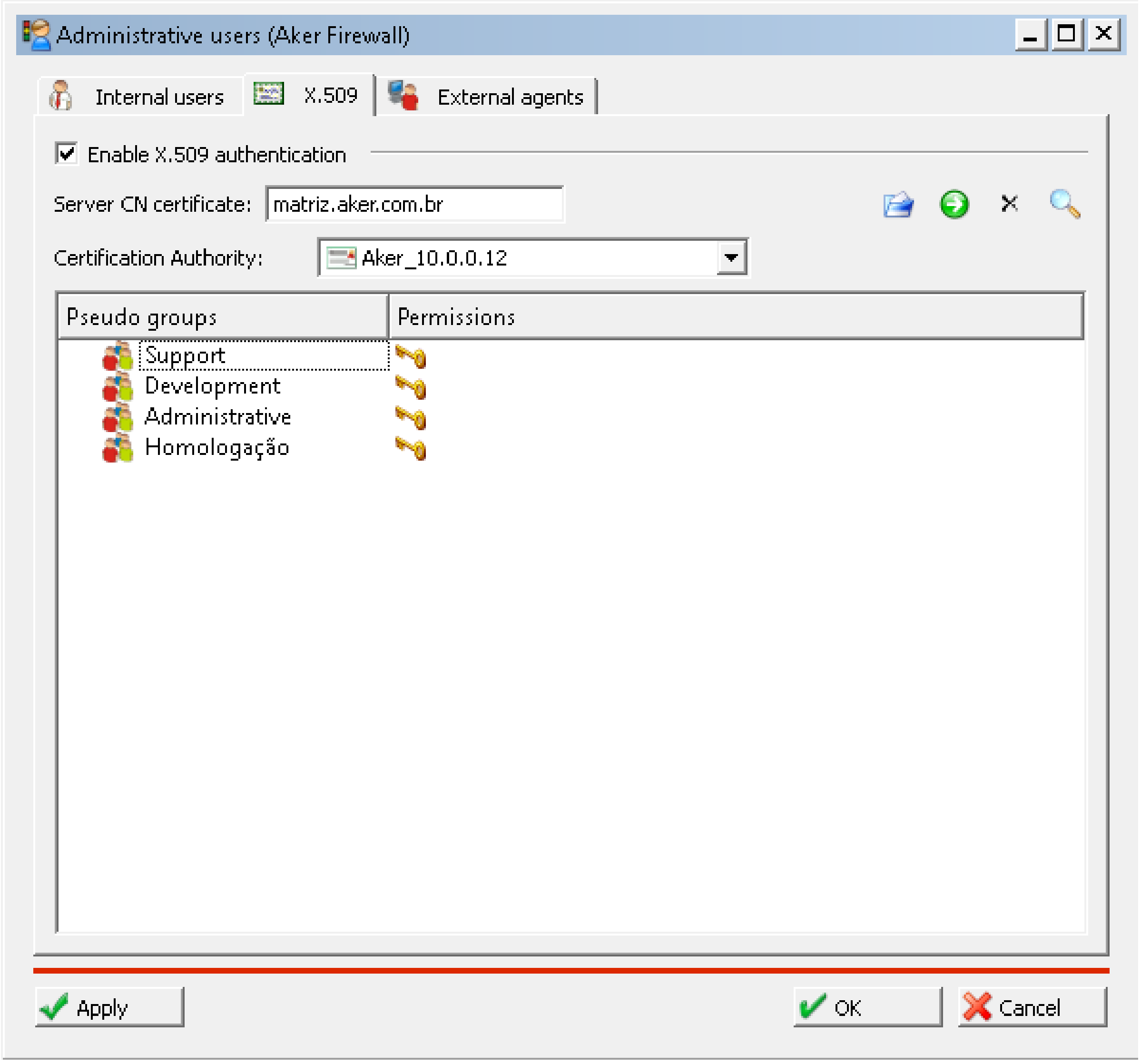
Entity

Entities are representations of the real world objects for Aker Firewall. Through them, computers, networks, services to be made available, among other. This option allows definition from which entity the user will connect to the firewall.

Sever fingerprint

This is a summary of the Aker Firewall digital certificate. This option allows the user to identify when there is a Firewall change which is usually connected.

X.509 Authentication Tab



☑ Enable X.509 authentication

Server CN certificate: matriz.aker.com.br

Certification Authority: Aker_10.0.0.12

Pseudo groups	Permissions
Support	🔑
Development	🔑
Administrative	🔑
Homologação	🔑

Image 115 – Authentication Administrator Users – X509.

This tab consists of the authentication method with the X.509 *Digital certificate*. The Digital Certificate can be considered the electronic (digital) version of an ID card; it associates a public key with the real identity of an individual, a server system or some other entity. A digital certificate is normally used to connect an entity to a public key. To ensure the integrity of the information contained in this file, it is digitally signed, in case of a Public Key Infrastructure (PKI), the certificate is signed by the Certificate Authority (CA) issuing it and in case of a Web of Trust model, such as PGP, the certificate is signed by the very entity itself and by others who claim to trust that entity. In both cases the signatures contained in a certificate are certifications made by an entity who claims to trust the data contained in that certificate.

A certificate normally includes:

- Information related to that entity to which the certificate was issued (name, email, CPF/CNPJ, PIS etc.);
- The public key related to the private key held by the entity specified in the certificate;
- Duration;
- The location of "revocation center" (a URL for CRL download, or a place for an OCSP query);
- The CA/entity signature(s) claiming that the public key contained in that certificate is in accordance with the information the certificate contains.

The default X.509 certificate is another common certificate format. All X.509 certificates follow the ITU-T X.509 international standard; therefore (theoretically) X.509 certificates created for an application may be used by any application that follows X.509.

A certificate requires someone to validate that a public key and the key owner’s name go together. With PGP certificates anyone may play the role of a validator. With X.509 certificates, the validator is always a Certificate Authority or someone assigned by a CA.

A X.509 certificate is a standard set collection of fields containing information about a user or device and their corresponding public keys. The X.509 standard defines which information goes to the certificate as well as describes how to encode this (data format). All X.509 certificates contain the following data:

The number of the X.509 version which identifies what standard is applied on the X.509 version for this certificate, what it affects as well as what information can be specified on it.

The certificate holder public key together with an identification algorithm, specify what encryption system belongs to that key and any associated parameters.

Below, there are the fields contained in the tab.

Enable X.509 authentication:

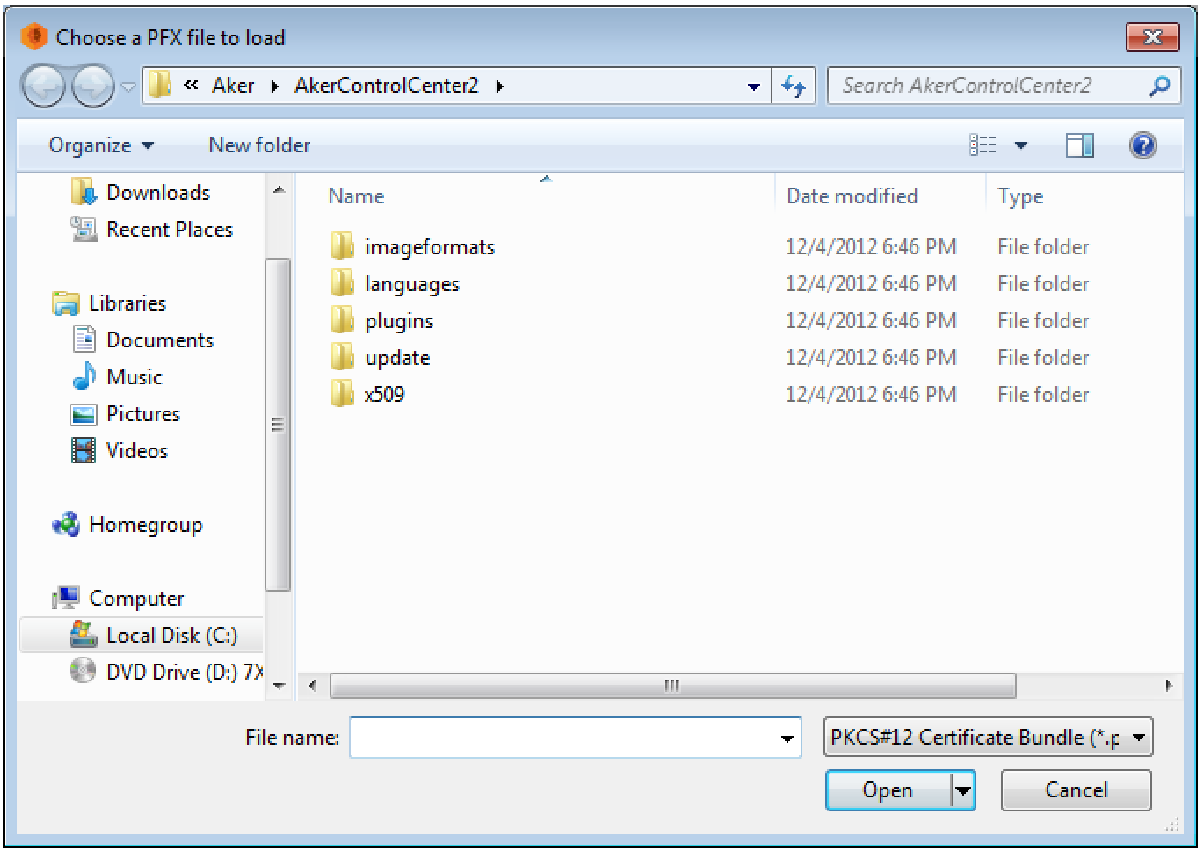
When selected, this option enables user authentications via digital certificate X.509.

Firewall certificate CN:

This option displays which certificate Aker Firewall is using in its authentication.

Import Certificate:

Clicking this icon allows the inclusion of a new certificate, meaning, the certificate registered on file is loaded and included to the firewall.


Choose a PFX file to load
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize ▾
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
File name:
PKCS#12 Certificate Bundle (*.p
Open
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder

Image 116 – Import certificate.

Just select the certificate and click on **“Open”**. On the following screen 3 requests will be made: **“Certificate Password”**, **“Password to save the private key”** and **“Confirm private key password”**. Click **“OK”**.

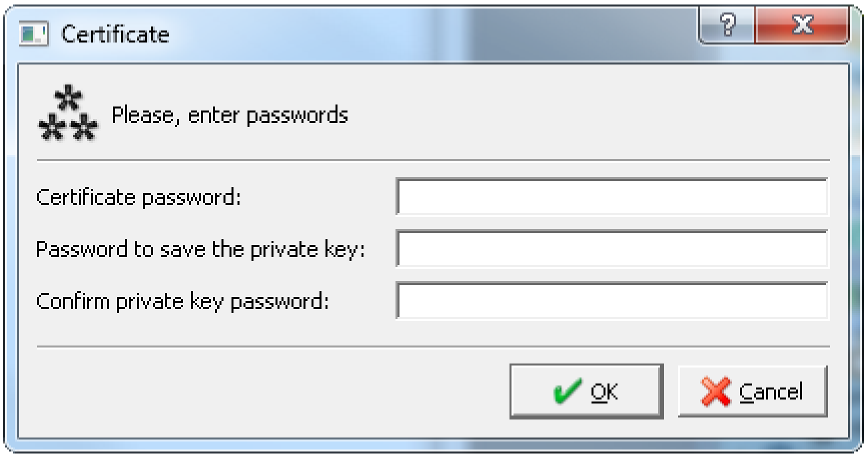
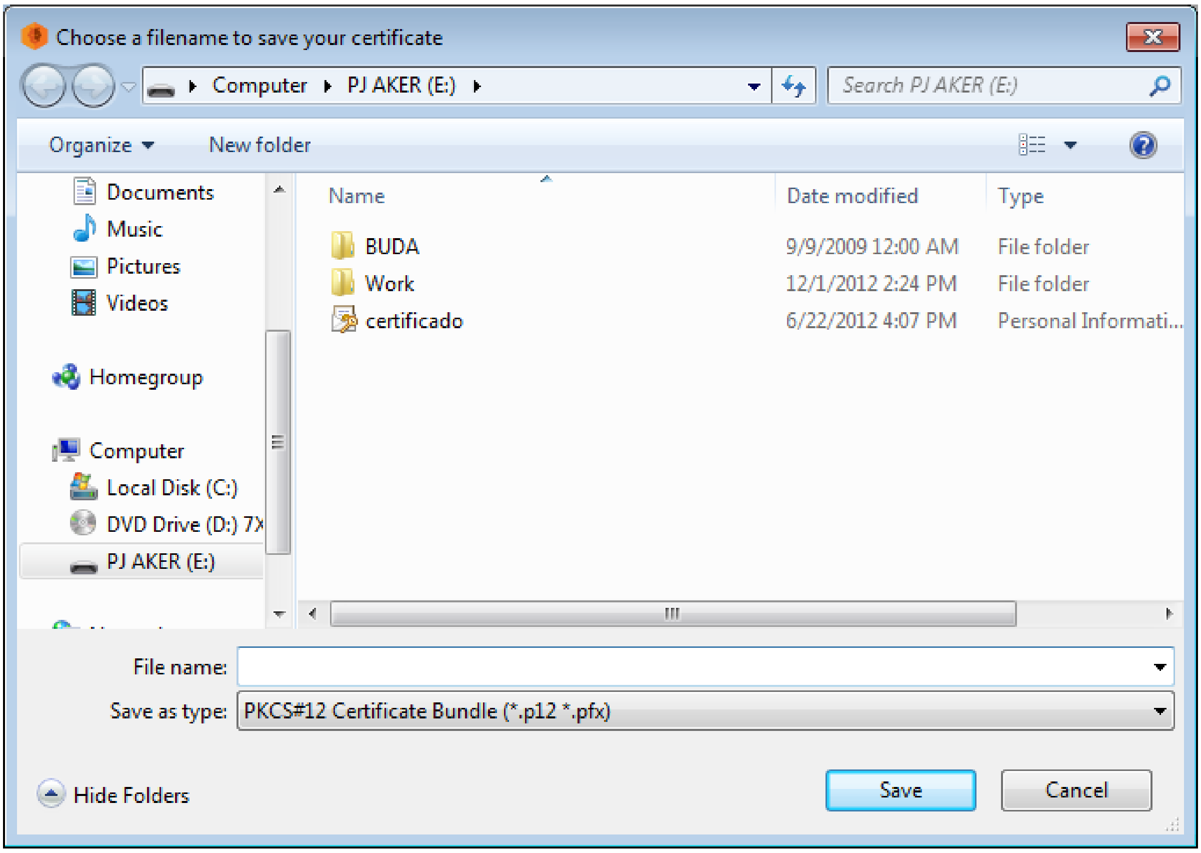

Certificate
Please, enter passwords
Certificate password:
Password to save the private key:
Confirm private key password:
OK
Cancel

Image 117 – Certificate (imported)

Export Certificate: Saves certificate data in order to transport it to a future application of this certificate. It copies the certificate.


Choose a filename to save your certificate
Computer ▸ PJ AKER (E:) ▸
Search PJ AKER (E:)
Organize ▾
New folder
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
PJ AKER (E:)
Name
Date modified
Type
BUDA
9/9/2009 12:00 AM
File folder
Work
12/1/2012 2:24 PM
File folder
certificado
6/22/2012 4:07 PM
Personal Informati...
Hide Folders
Save
Cancel

File name:

Save as type: PKCS#12 Certificate Bundle (*.p12 *.pfx)

Image 118 – Export certificate

Choose and click on **“Save”.**

On the following screen 4 requests will be made: **“Password to save certificate”**; **“Confirm certificate password”**; **“Password to save private key”**; and **“Confirm private key password”**. Click **“OK”**.

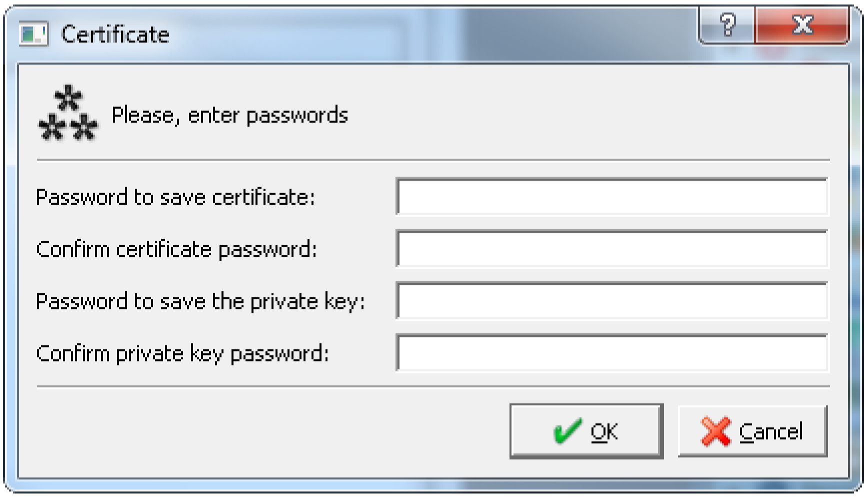
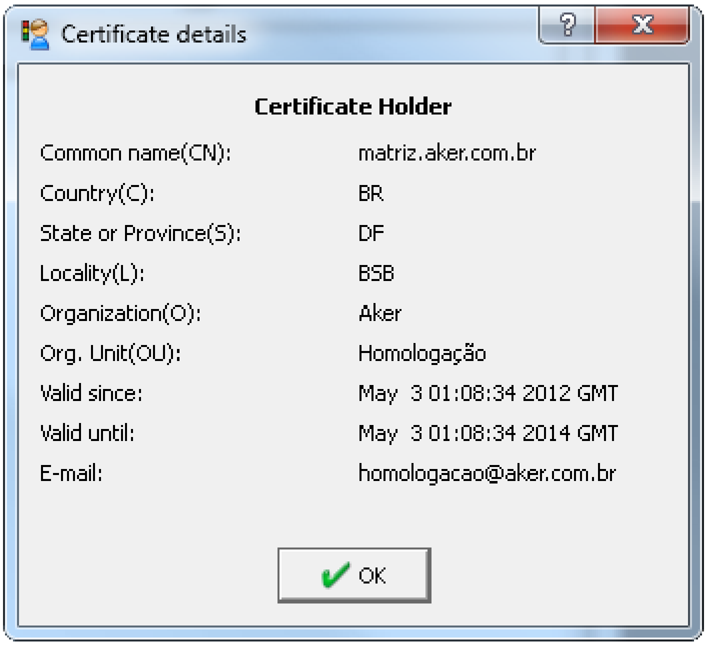

Certificate
Please, enter passwords
Password to save certificate:
Confirm certificate password:
Password to save the private key:
Confirm private key password:
OK
Cancel

Image 119 – Certificate (exported).

Remove Certificate: Clicking this icon deletes the included certificate. In this way Aker Firewall remains without a certificate.

Display certificate details: Displays all information the enabled certificate contains.


Certificate details
OK

Certificate Holder

Common name(CN): matriz.aker.com.br
Country(C): BR
State or Province(S): DF
Locality(L): BSB
Organization(O): Aker
Org. Unit(OU): Homologação
Valid since: May 3 01:08:34 2012 GMT
Valid until: May 3 01:08:34 2014 GMT
E-mail: homologacao@aker.com.br

Image 120 – Certificate Details

Certificate Authority:

The certificate authority (CA) shall guarantee to the user, through signing and issuing its certificates, that such entities really are who they claim to be. Therefore, the CA has a role of ensuring correspondence between an entity and a public key of a determined entity, being aware that such public key corresponds to a private key under the exclusive guard of this entity.

For such, the CA shall be capable of performing certificate issuing processes, checking validation, storage, publication or online access, revocation and filing for future verification.

Therefore, a certificate authority is made up of a complete computer system, able to communicate the process and store. In addition to this, not only communications related to this system but also the system itself shall be protected and its identity guaranteed these needs are met by means of the publication of a public key owned by the certificate authority. Since this key shall also be guaranteed with a digital certificate, certificate authorities, in general, deposit their public Keys alongside other certificate authorities, forming a certification structure from where some CAs work as certificate authorities for other CAs.

This option selects a certificate authority which the user is bound.

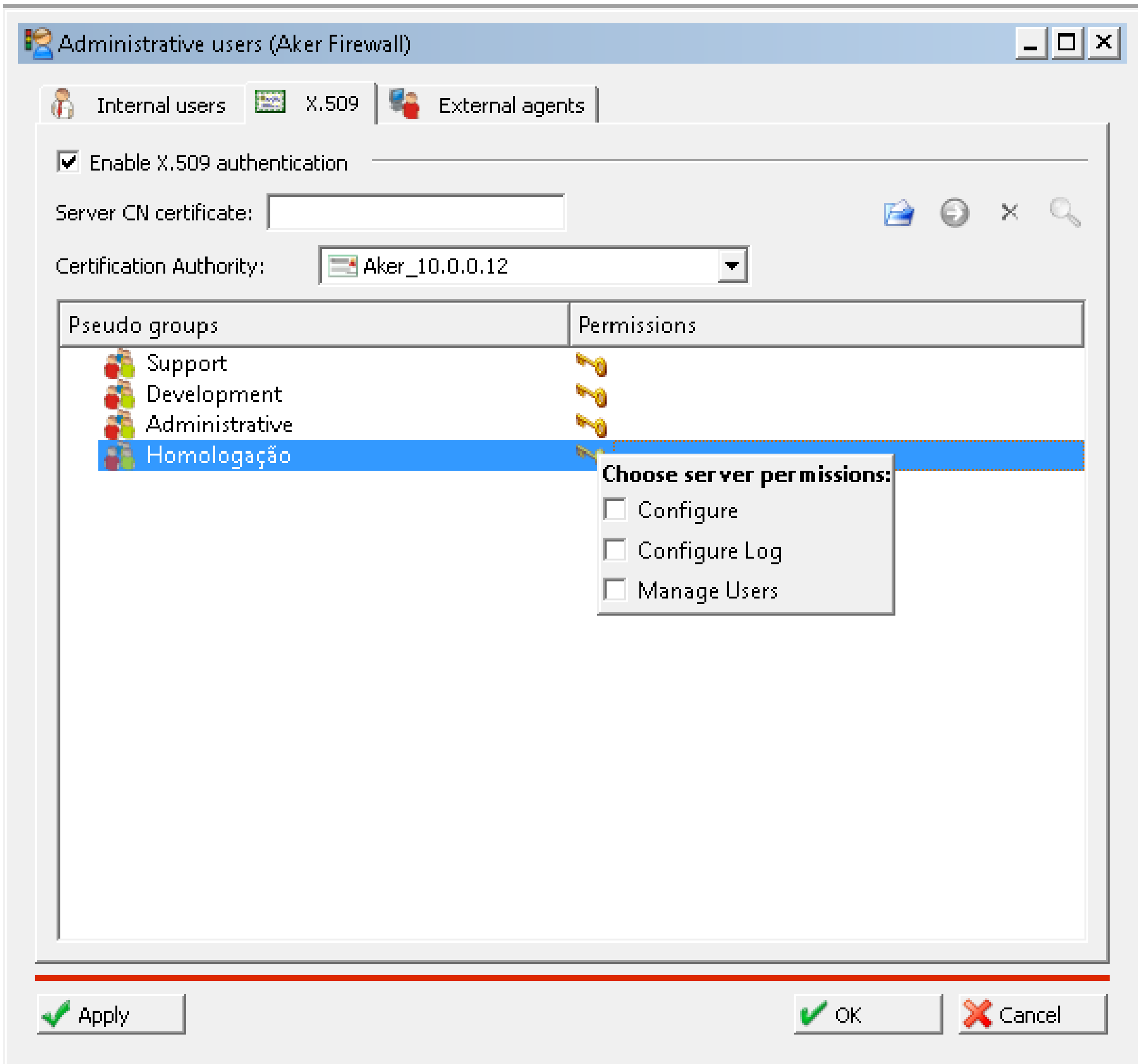
Pseudo Group

It corresponds to certificate groups associated to the selected certificate authority. The **"Pseudo Group"** field is not editable.

Permissions

The **"Permissions"** field is editable, enabling each selected CA to relate permissions for each group.

Under this option, once a Certificate Authority has been chosen and the access levels/permissions have been defined for each group, in case of a CA switch, all permissions related to the previous CA will be lost.


Administrative users (Aker Firewall)
Internal users
X.509
External agents
Pseudo groups
Permissions
Choose server permissions:
Apply
OK
Cancel

☑ Enable X.509 authentication

Server CN certificate:

Certification Authority: Aker_10.0.0.12

Pseudo groups	Permissions
Support	
Development	
Administrative	
Homologação	

Choose server permissions:

☐ Configure

☐ Configure Log

☐ Manage Users

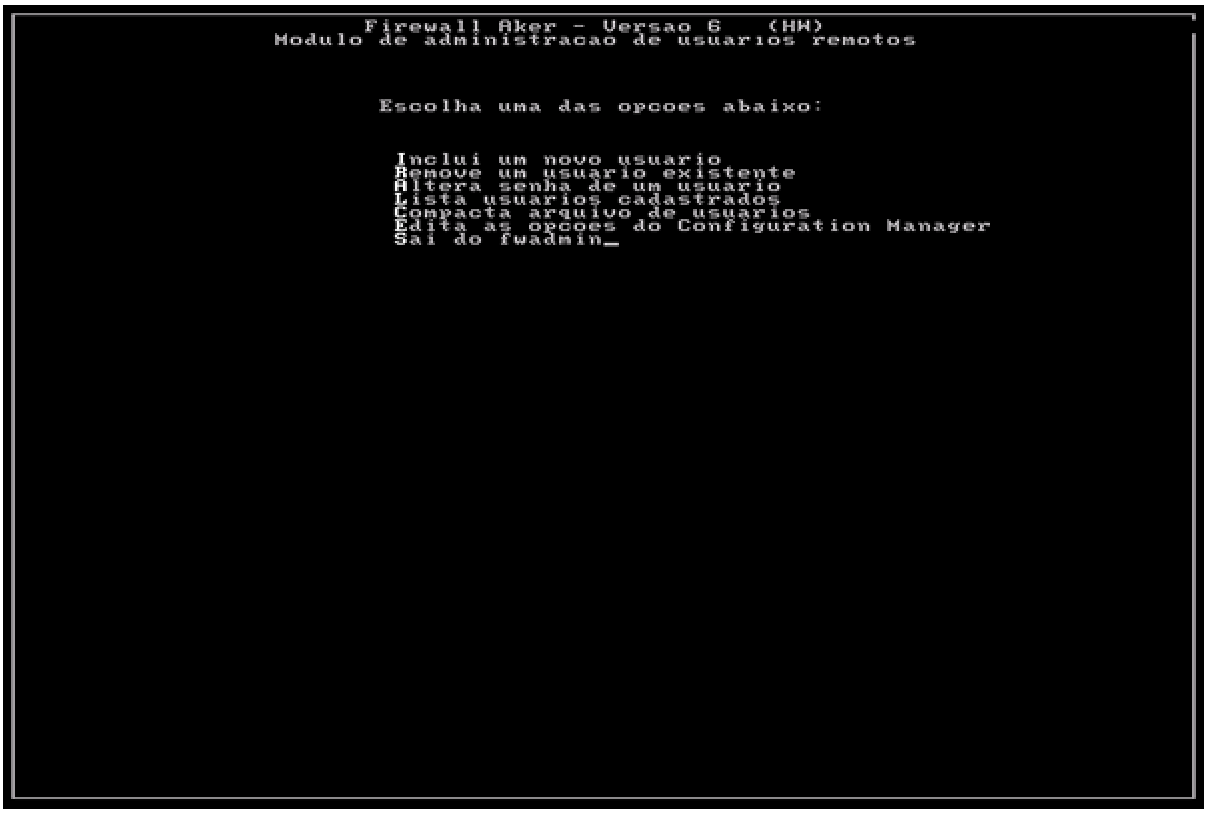
Image 121 – Server choices option.

4.2. Using the text interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action)*. The only non-available function is the *changing user permissions*. This text interface, as opposed to most character oriented interfaces on Aker Firewall, is interactive and does not receive line command parameters.

Program location: /etc/firewall/fwadmin

When you run the program the following screen will be displayed:

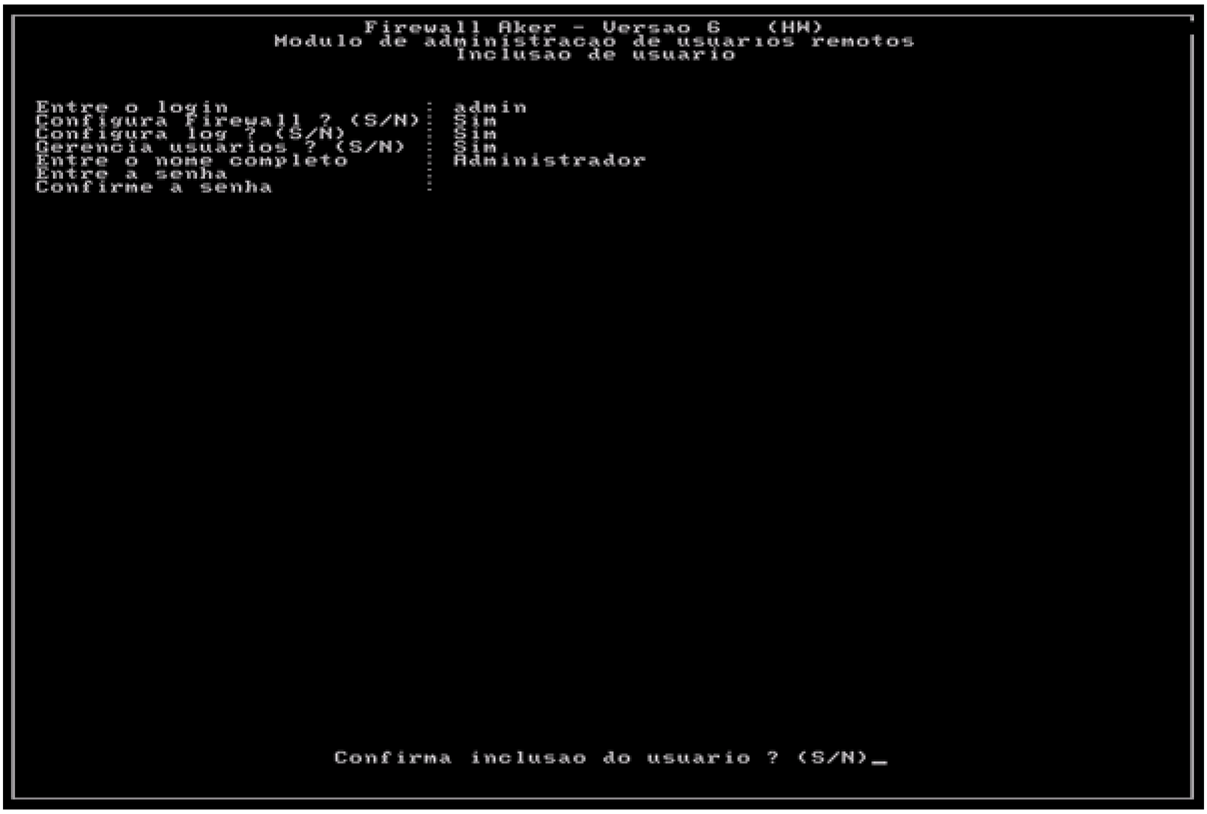


```
              Firewall Aker - Versao 6   (HW)
        Modulo de administracao de usuarios remotos


                   Escolha uma das opcoes abaixo:


                    Inclui um novo usuario
                    Remove um usuario existente
                    Altera senha de um usuario
                    Lista usuarios cadastrados
                    Compacta arquivo de usuarios
                    Edita as opcoes do Configuration Manager
                    Sai do fwadmin_
```

Image 122 – Using the text interface to run the program.

To run any of the available options, just type the letter in bold. Each option is described below:

- **Including new user:** This option includes a new user that may manage Aker Firewall remotely. When selected, a screen requiring few users’ information is displayed. After all information is filled in a confirmation for user inclusion is displayed.

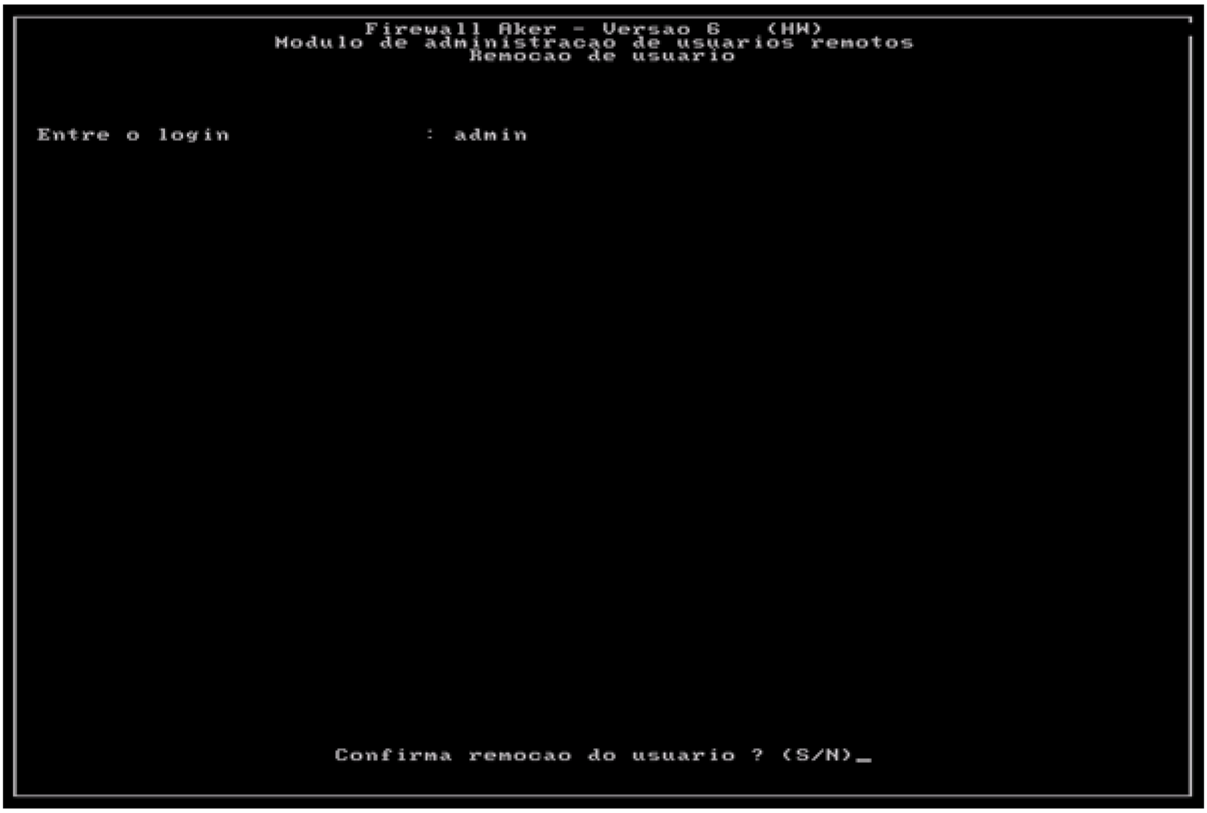


```
                       Firewall Aker - Versao 6   (HW)
              Modulo de administracao de usuarios remotos
                          Inclusao de usuario

Entre o login                    :  admin
Configura Firewall ? (S/N):  Sim
Configura log ? (S/N)         :  Sim
Gerencia usuarios ? (S/N)  :  Sim
Entre o nome completo      :  Administrador
Entre a senha                  :
Confirme a senha              :




                 Confirma inclusao do usuario ? (S/N)_
```

Image 123 – Running the program to include users as Aker Firewall administrators.

To proceed with inclusion, press **Y**. To abort operation, press **N**.

- **Removing registered user:** This option deletes a registered user from the system. The selected user log to be removed is necessary. Next, there is a confirmation so the operation can be performed.

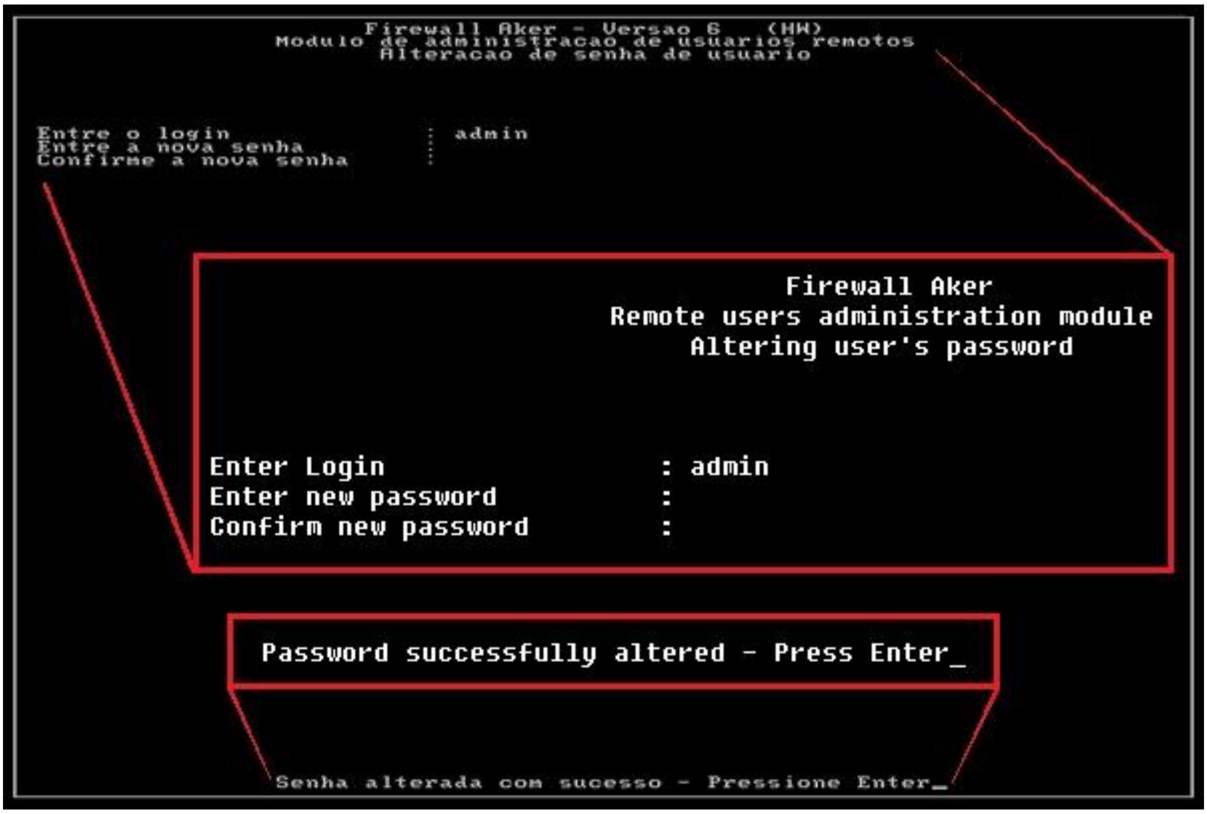


```
                     Firewall Aker - Versao 6   (HW)
               Modulo de administracao de usuarios remotos
                           Remocao de usuario


 Entre o login              : admin




                   Confirma remocao do usuario ? (S/N)_
```

Image 124 – Running the program to delete users.

To proceed with removal, press **Y**. To abort operation, press **N**.

- **Changing a user password**: This option changes the password of a registered user in the system. The user login whose password will be altered is necessary. Type in the new password. Next, there is a confirmation so the operation can be performed.

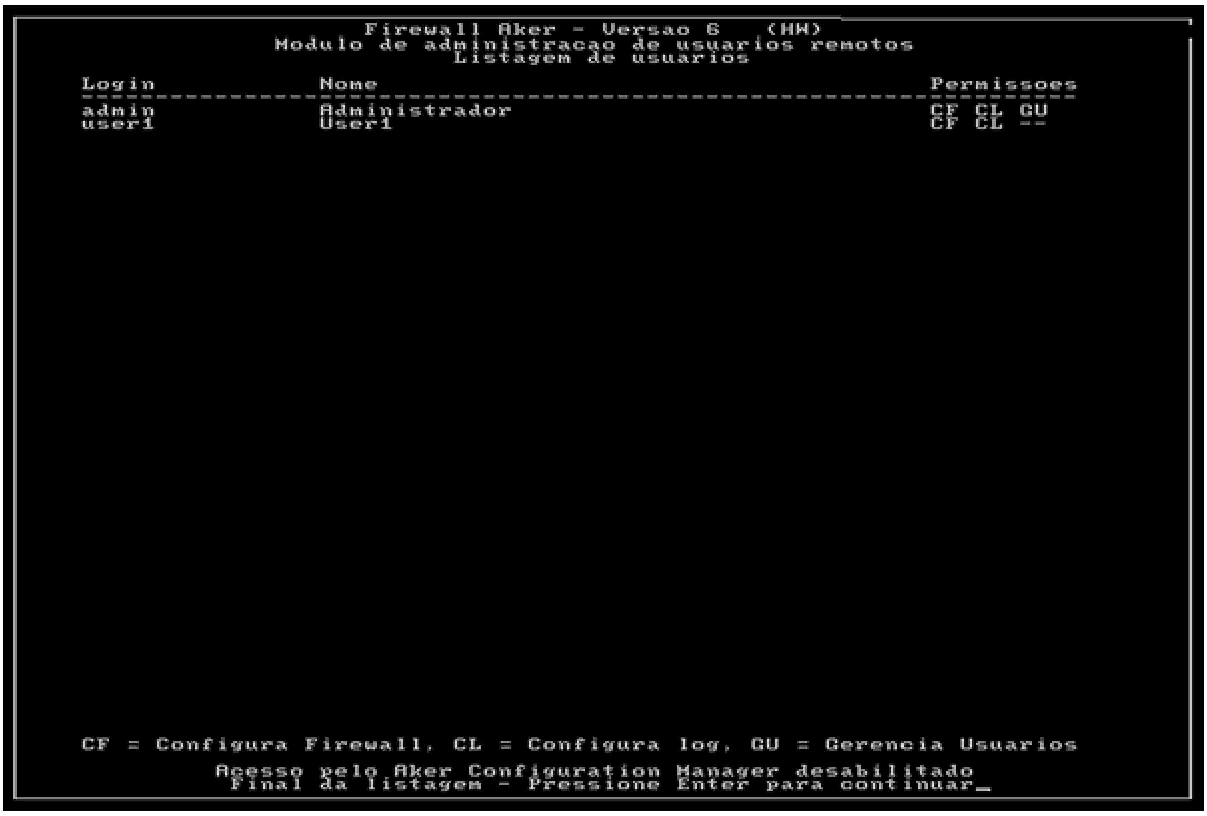


```
              Firewall Aker - Versao 6   (HW)
        Modulo de administracao de usuarios remotos
             Alteracao de senha de usuario

Entre o login               : admin
Entre a nova senha          :
Confirme a nova senha       :

        Senha alterada com sucesso - Pressione Enter_
```

```
                    Firewall Aker
       Remote users administration module
           Altering user's password

Enter Login                 : admin
Enter new password          :
Confirm new password        :

Password successfully altered - Press Enter_
```

Image 125 – Running the program to alter a user’s password.

- **List of users:** This list of registered users displays all names and permissions of all authorized users to administrate the firewall remotely. An example of such listing of users follows below:



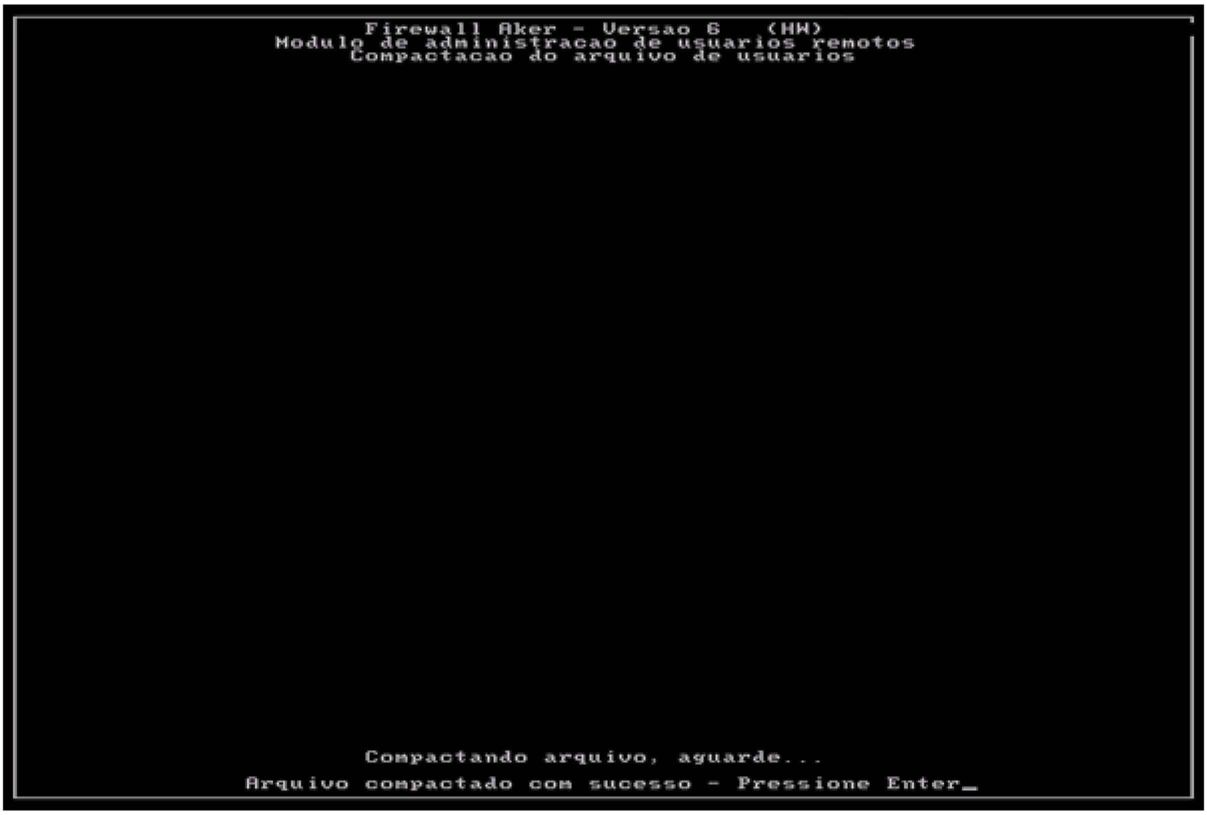
```
                   Firewall Aker - Versao 6   (HW)
             Modulo de administracao de usuarios remotos
                         Listagem de usuarios

Login           Nome                                     Permissoes
-------------------------------------------------------------------
admin           Administrador                            CF CL GU
user1           User1                                    CF CL --













CF = Configura Firewall, CL = Configura log, GU = Gerencia Usuarios

         Acesso pelo Aker Configuration Manager desabilitado
          Final da listagem - Pressione Enter para continuar_
```

Image 126 – Users listing

The field Permissions consists of 3 possible values: CF, CL, e GU, which respectively correspond to these following permissions: Configure Firewall, Configure Log and Manage Users. If the user has a permission, it will be displayed same as the code above, otherwise it will show the value, indicating that the user does not have it.

- **Compress user file:** This option is not present in the Remote Interface, and it is not used often. It is used to compress the user file, removing the unused entries. It should be used only when there is a large number of users who have been removed from the system.

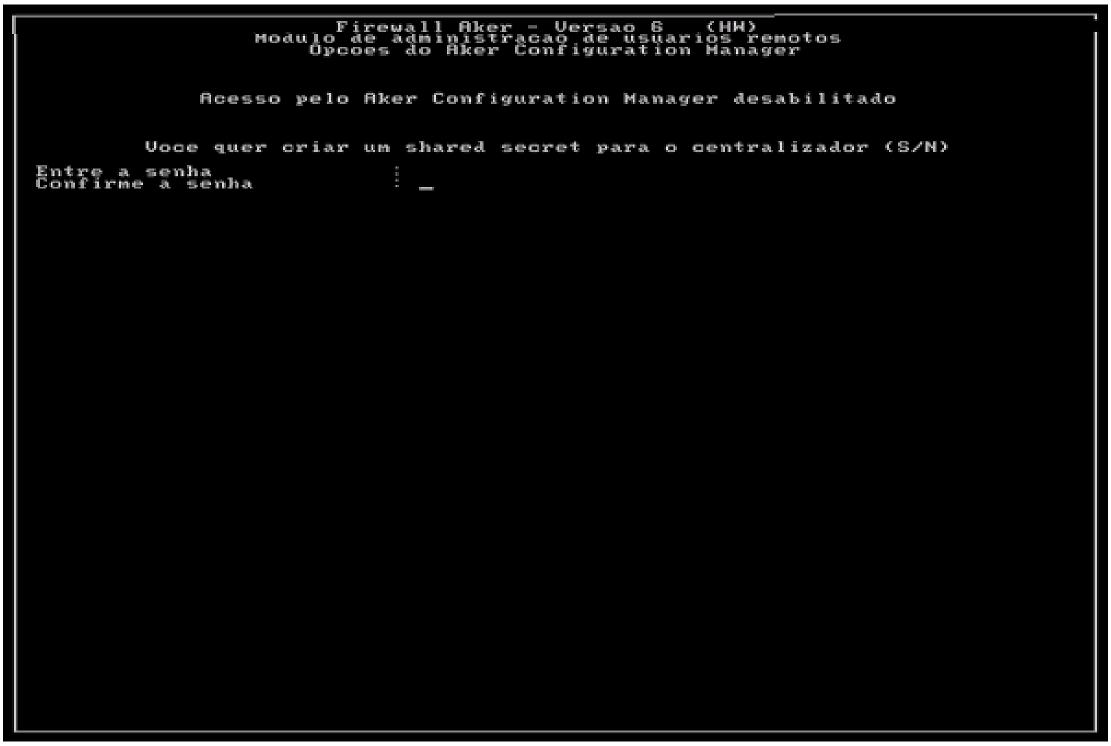
After being selected the file will be compressed and by the end of the process a message will be displayed, indicating that the operation was completed (the file compressing is normally really fast, taking Just few seconds)



```
                 Firewall Aker - Versao 6   (HW)
          Modulo de administracao de usuarios remotos
              Compactacao do arquivo de usuarios

                 Compactando arquivo, aguarde...
          Arquivo compactado com sucesso - Pressione Enter_
```

Image 127 – The program compression to show the user file compression.

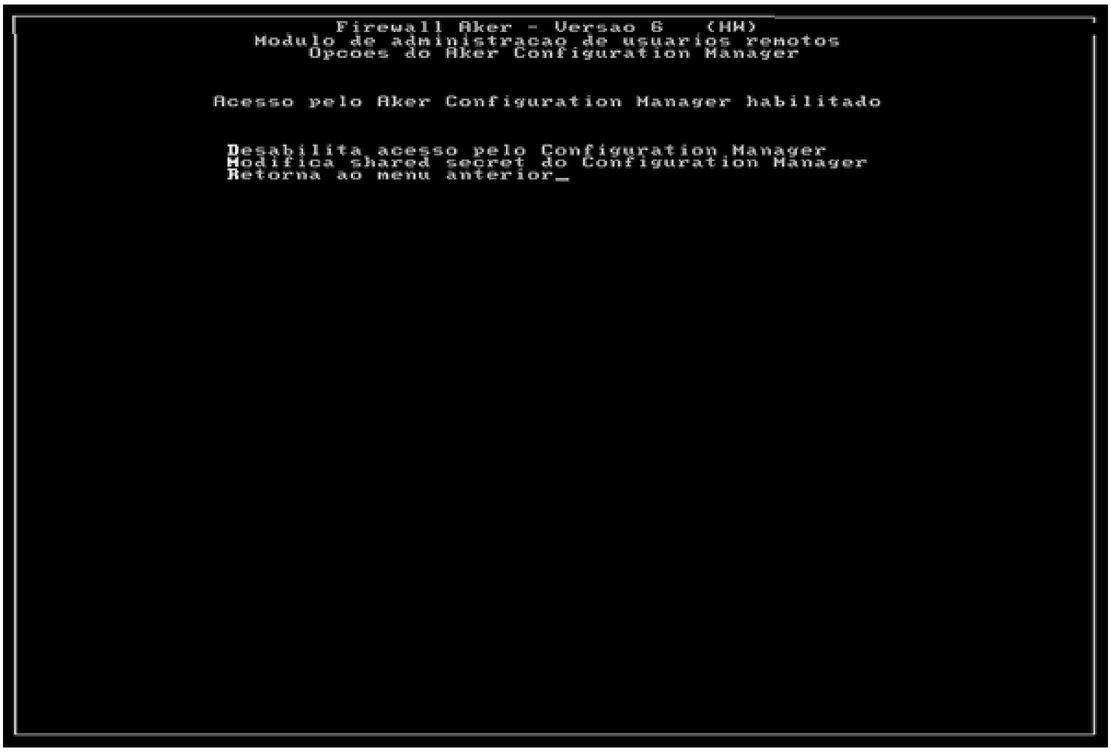
- **Edit the Configuration Manager options:** This option allows changing Aker Configuration manager setup. It is possible to enable/disable access to Aker Firewall via Configuration Manager and change the shared secret. . If the access to the Firewall is disabled, a screen will be displayed, requesting the shared secret creation. It is necessary to fill the password and confirmation.



```
                    Firewall Aker - Versao 6    (HW)
               Modulo de administracao de usuarios remotos
                  Opcoes do Aker Configuration Manager


           Acesso pelo Aker Configuration Manager desabilitado


        Voce quer criar um shared secret para o centralizador (S/N)
Entre a senha                     :
Confirme a senha                  : _
```

Image 128 – Aker Configuration Manager setup edition.

If the Firewall access is enabled, a new setup options will be displayed:

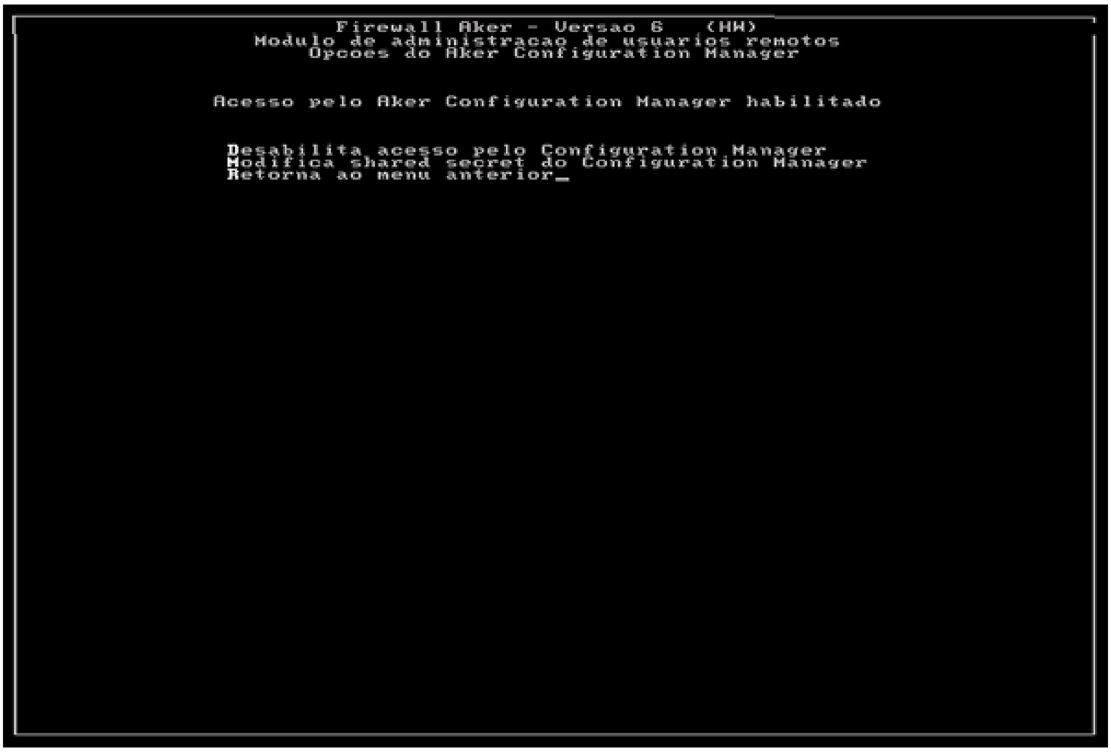


```
               Firewall Aker - Versao 6    (HW)
         Modulo de administracao de usuarios remotos
             Opcoes do Aker Configuration Manager


      Acesso pelo Aker Configuration Manager habilitado


       Desabilita acesso pelo Configuration Manager
       Modifica shared secret do Configuration Manager
       Retorna ao menu anterior_
```

Image 129 – Aker Configuration Manager setup (Enabled Firewall).

- **Disable access through Configuration Manager:** When selecting this option, will not be possible to Access the Aker Firewall through Configuration Manager, until the user enable the access.

- **Modify Configuration Manager shared secret:** Allows changing a shared secret. It is necessary entry a new password with its confirmation.

- 

```
                Firewall Aker - Versao 6    (HW)
          Modulo de administracao de usuarios remotos
              Opcoes do Aker Configuration Manager

       Acesso pelo Aker Configuration Manager habilitado

        Desabilita acesso pelo Configuration Manager
        Modifica shared secret do Configuration Manager
        Retorna ao menu anterior_
```

Image 130 – Aker Configuration Manager Setup edition (Disable, modify return).

- **Exit the fading:** This option ends the program ***fading*** and returns to the command line.

Configuring System Parameters

5. Configuring the system parameters

This chapter will show how to setup the variables that will affect in the entire system results. These configuration parameters operate in ways like the security, system log and connections' downtime.

5.1. Using the Remote Interface

To gain access to the Configuration Parameters, follow the steps below:

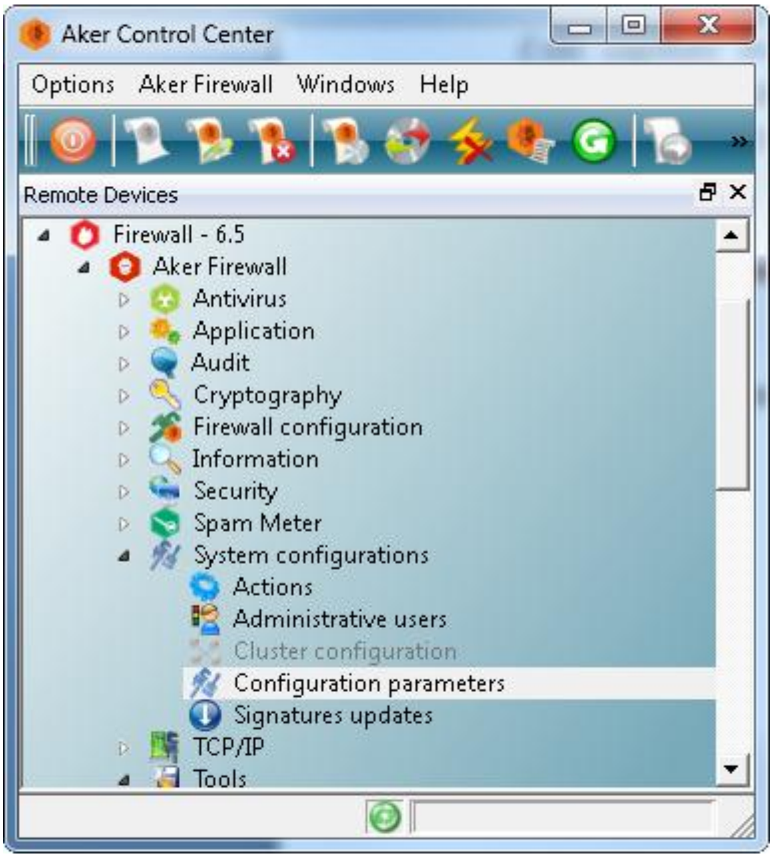

Aker Control Center
Options
Aker Firewall
Windows
Help
Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
Actions
Administrative users
Cluster configuration
Configuration parameters
Signatures updates
TCP/IP
Tools

Image 131 – Configuration parameters

- Click on the *System configurations* menu in the Firewall you wish to configure.
- Select *Configurations parameters*

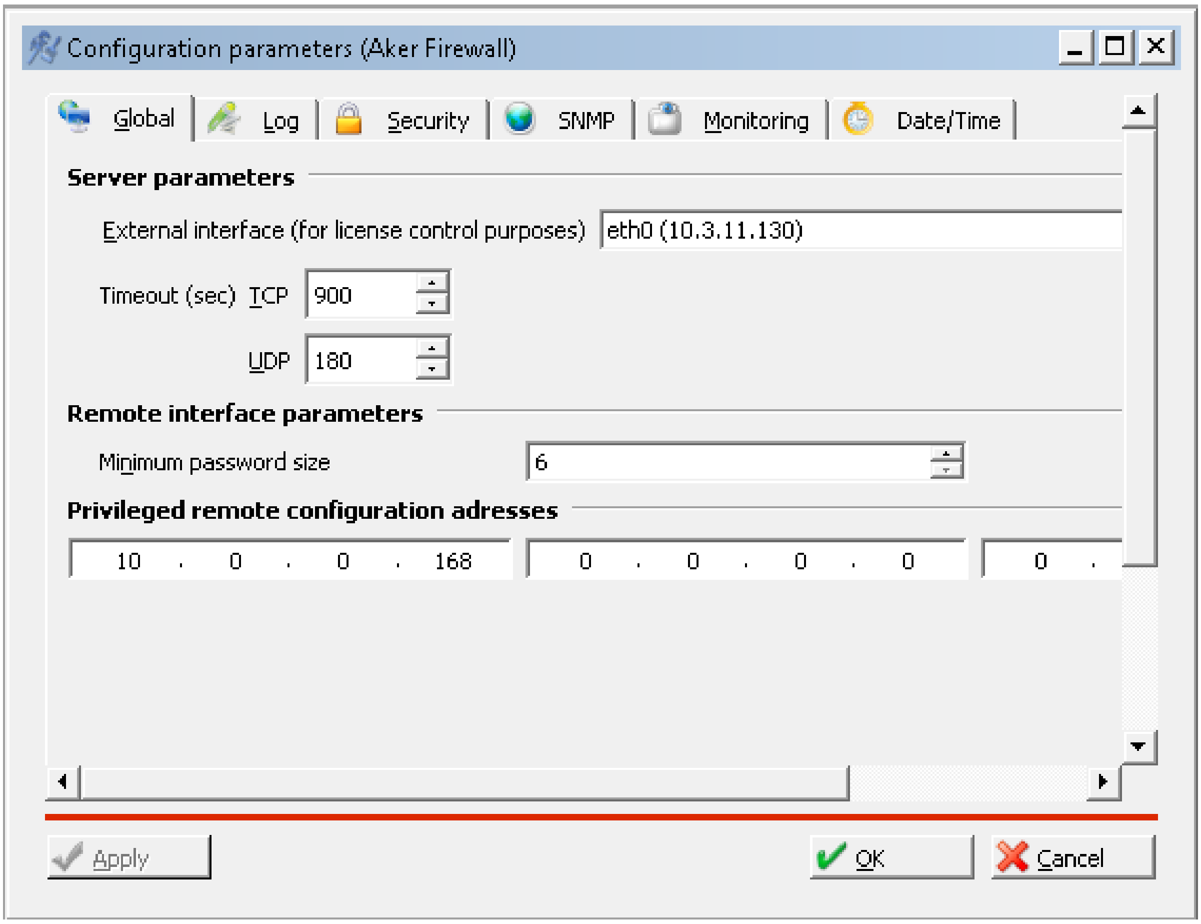
The window Configuration parameters

- The ***OK*** button will make the Configuration parameters window close and the made changes be applied.

- The ***Cancel*** button will close the Window, but the changes will not be applied.
- The ***Apply*** Button will save all made changes to the Firewall, but will keep the Window open.

Parameters meaning

Global Tab


Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time
Apply
OK
Cancel

Server parameters

External interface (for license control purposes): eth0 (10.3.11.130)

Timeout (sec) TCP: 900

UDP: 180

Remote interface parameters

Minimum password size: 6

Privileged remote configuration adresses

10 . 0 . 0 . 168

0 . 0 . 0 . 0

0 .

Image 132 – Configuration parameters (Global Tab)

In this window, theses parameters will be used by the *stateful inspection* and by the address translation

External interface (For license control purposes): Defines the name of the Firewall External interface. Connections that shall come via this interface do not count in the license.

Default value: Configured during the firewall installation by the administrator.

Time limit TCP: Defines the maximum time, in seconds, that the TCP connection can remain without traffic and still be considered by the firewall. Its value may vary from *0 to* 259200 (72 hours).

Default value: ***900*** seconds.

Time limit UDP: Defines the maximum time, in seconds, that the UDP connection can remain without traffic and still be considered by the firewall. Its value may vary from 0 to 259200 (72 hours)

Default value: ***180*** seconds.

These fields are of vital importance for firewall proper operation. Values too high might cause security problems for services, based in the UDP protocol, values too high will make the system use more memory and it will become slow. Values too low might cause Constant falls from session and the malfunction of some services

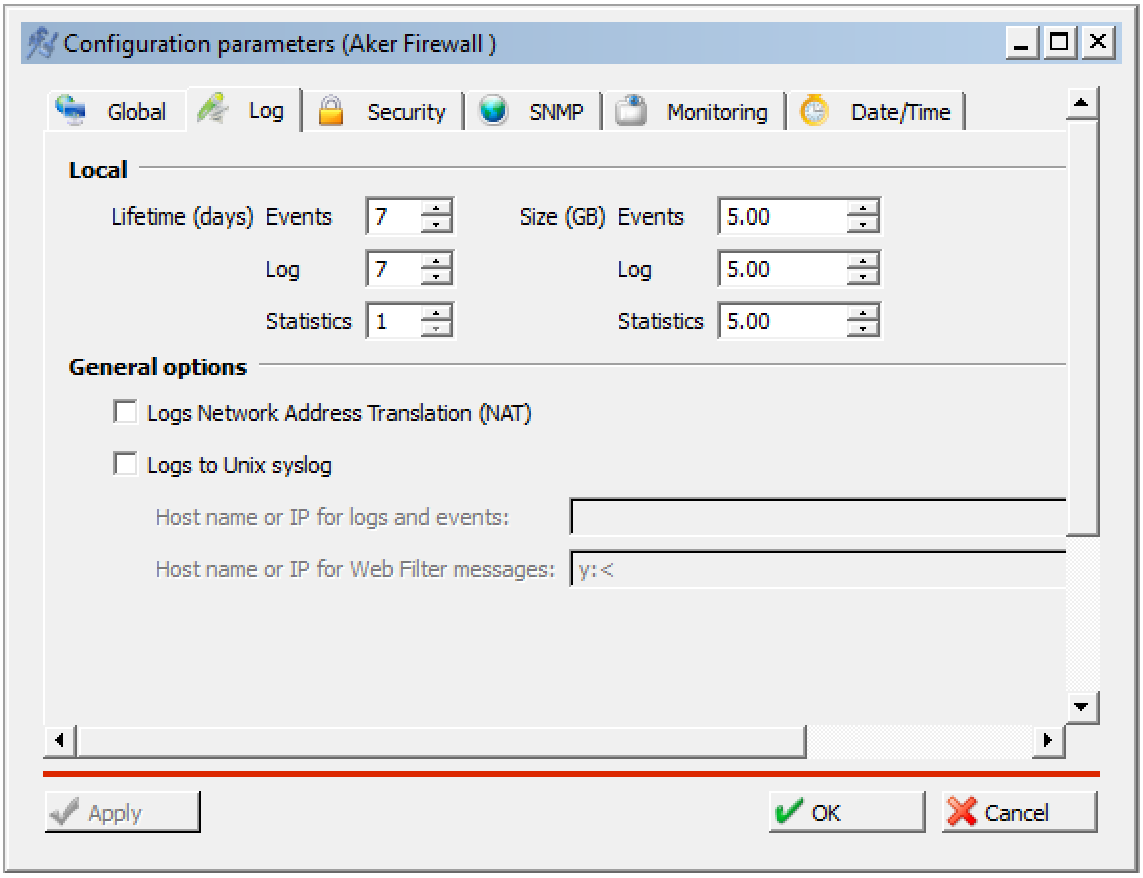
Minimum password size: Defines the minimum number of characters that the administrators' passwords shall have to be accepted by system. Its value may vary between 4 and 14 characters.

Default value: **6** characters.

It is important that this value is the largest as possible, to avoid the use of passwords which can be easily broken.

Privileged remote configuration addresses: They are addresses that independently of rules and extrapolating limits of license can administrate the firewall (this is connecting in the port 1020). They work was a preventive measure for the firewall anti-lock, once it can only be configured through the Text Interface.

Log tab



Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time
Apply
OK
Cancel

Local

Lifetime (days) Events 7 — Size (GB) Events 5.00

Log 7 — Log 5.00

Statistics 1 — Statistics 5.00

General options

☐ Logs Network Address Translation (NAT)

☐ Logs to Unix syslog

Host name or IP for logs and events:

Host name or IP for Web Filter messages: y:<

Image 133 – Configuration parameters: Log tab

Local: Indicates that the log/events/statistics shall be saved in a local disk, in the host where the firewall is running.

Lifetime (days) in the log / events / statistics: The firewall log register, events and statistics are kept in daily files. The configuration defines the maximum number of files that will be kept by the system, in the local log. The possible values go from 1 to 365 days.

Default value: ***7*** days

Size (GB) / events / log / statistics: The files (log, events or statistics) will be limited in disk size, i.e. whenever the logs exceed the maximum size, the older files will be deleted.

Example of the new firewall logs rotation.

	PREVIOUS	PRESENT
Rotation period	Daily	Hourly or when the file exceeds the maximum size configured by the administrator.
Files exclusion control	When the files exceed the time limit configured by the administrator.	When the files exceed the time limit configured by the administrator.

Example:

Network environment configuration:

Time limit: 07 days maximum log size of *2,4 GB*

100 MB of log files are generated per hour.

On the *01st day* at 11:59, there will be approximately *2,4 GB* of log files.

On the 02nd day at midnight, the firewall will rotate the logs.

This action will cause the first log file of *100 MB*, created on the first day be deleted from the hard drive, so this log file will have *2,3 GB* of log files.

After it, the firewall has received a *flood attack* and has begun to generate *3,4 GB* of log per hour.

When the file log (ONLY THE FILE WHICH IS BEING WRITTEN, NOT COUNTING THE OTHER FILES) reach *2,4 GB* (at this moment the directory will have *4,7 GB* of log), the firewall will rotate the logs excluding *ALL* log registry, including the *2,4 GB* file. Following a new file will be created and the logs will be saved in this new file.

06 days, 23 hours and 59 minutes have passed and the firewall has created several log files, reaching a total size of *1,000160217 GB*. At midnight, after the *07th* day the firewall has rotated the logs, excluding only the file of *1 GB*, created a week ago, and leaving only *0,000160217* of log files.

In the example above, it is used the *log*, but the functioning is the same regarding to the *events* and *statistics*. The rotation is not instantaneous. It occurs in two manners: hourly or when the file which the registers are being saved, exceeds the size configured by the administrator.

In case the of remote log using, these options are going to be disabled and shall be configured in the remote server itself.

Remote: This option shows that the log/events/statistics shall be sent to a remote log sever instead of be saved in the local disk.

Remote server: This option indicates to the remote log server, which log/events/statistics it will be sent to. So the control of many firewalls can be centered making the auditing easier.

Log address translation (NAT): Enables the register in the system log of address translation made by the firewall.

Default value: ***Address translation should not be logged***

Even with this option active, only the converted packages Will be logged through the address translation 1:N and N:1. The address translations through others types of rules will not be registered.

This option's activation does not bring any important information and it shall be used only to tests or trying to solve problems

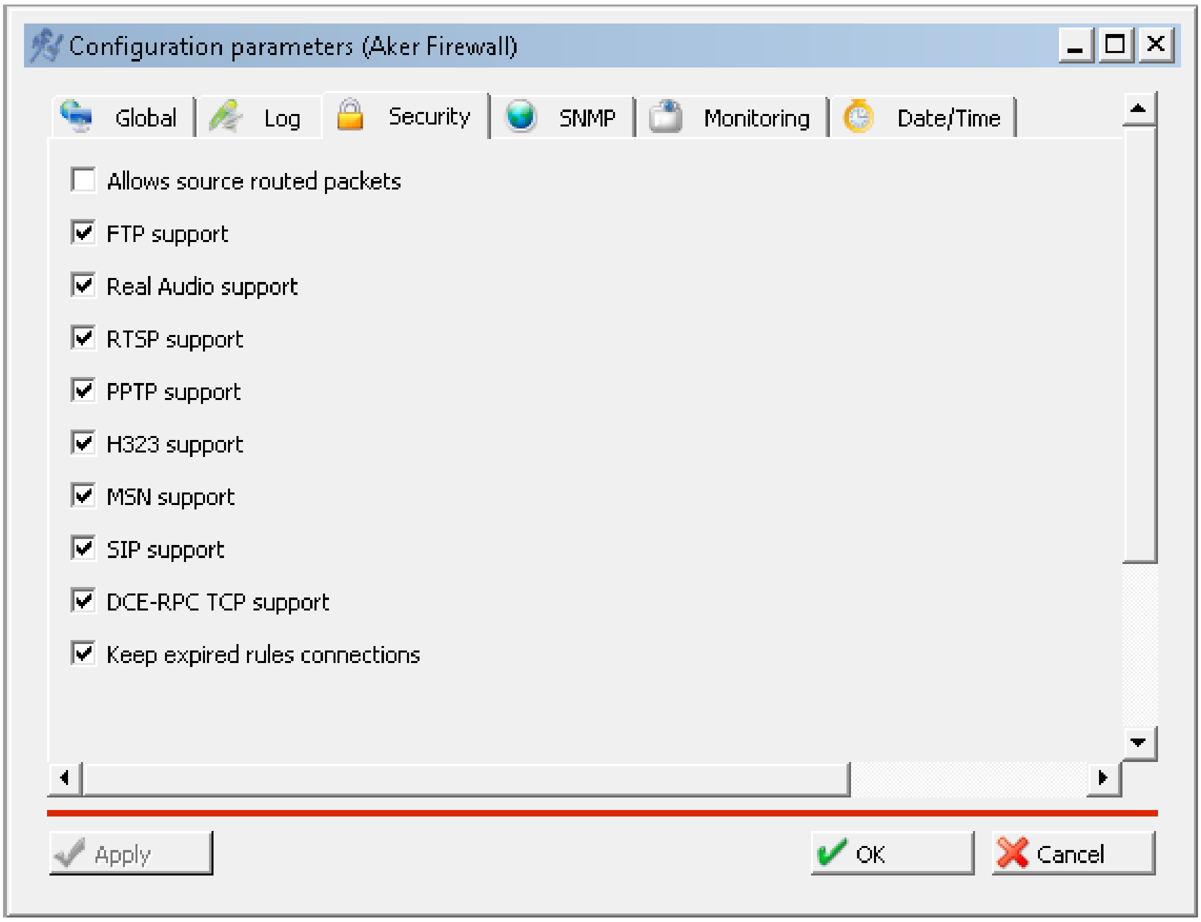
Log UNIX syslog: Enables the sending of firewall log and events to the UNIX daemon log, the *syslogd.*

Default value: ***Does not send log to the syslogd***

By enabling this option, the log registers will be sent to ***local 0*** *queue* and the events will be sent to ***local 1*** *queue*.

This option does not change anything in the internal log record and the events made by the firewall itself.

Security Aba


Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time
Apply
OK
Cancel

☐ Allows source routed packets

☑ FTP support

☑ Real Audio support

☑ RTSP support

☑ PPTP support

☑ H323 support

☑ MSN support

☑ SIP support

☑ DCE-RPC TCP support

☑ Keep expired rules connections

Image 134 – Configuration parameters: Security tab

Security parameters

Allows source routed packets: Enables the passing of packets that have the register route option or directed routing. If this option is unchecked, the packets with some of these options will not be able to pass through.

Default value: ***Packets IP directed will not be allowed.***

The acceptance of packets with route to source can cause a serious security failure. Unless there is a specific reason to let them pass through, this option shall remain unchecked.

- **FTP Support:** Enables specific support for FTP protocol.

Default value: **FTP *Support is enabled***

This parameter allows the FTP protocol works transparently to all hosts, clients and servers, internal or external. Unless intend to use FTP through the firewall, this option shall be unchecked.

.

- **Real Audio support:** Enables the support to the protocols Real Audio and Real Video.

Default value: ***Real Audio support is enabled.***

This parameter allows the Real Audio / Real Video protocol to work transparently using TCP and UDP connections. Unless intend to use Real Audio, or use it with TCP connections, this option shall be checked.

- **RTSP support:** Enabled the support to RTSP protocol.

Default value: ***RTSP support is enabled***.

The RTSP (Real Time Streaming Protocol) is a protocol that acts at the level of application that allows the controlled delivery of data in real-time, like audio and video. Data sources can include programs live (with audio and video) or some stored content (events pre-saved). It is projected to work with protocols like RTP, HTTP or any other that supports the continuous media about the Internet. It supports multicast traffic like unicast. In addition, it also supports interoperability between clients and servers from different manufacturers. This parameter allows it to work transparently using TCP and UDP connections.

- **PPTP Support:** Enable the support to protocol PPTP of Microsoft

Default value: ***PPTP support is enabled.***

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products.

- **H323 Support:** Enables the support to protocol H.323

Default value: ***H323 support is enabled.***

The H.323 is a protocol that allows the implementation of voice about IP (VOIP) and it is supported by most devices with this purpose. This parameter allows protocol H.323 traffic normally through it, even with the address translation (NAT) enabled.

Some applications may not work with the H323 support enabled.

- **MSN support:** Enables the support to MSN Messenger

Default value: ***MSN Messenger support is enabled.***

The MSN Messenger is a protocol of IM (instant messaging) that allows the communication between two or more people at the same time. This parameter allows MSN protocol be controlled through the Access profiles.

- **SIP support:** Enables the support to SIP support.

Default value: ***SIP support is enabled****.*

The **SIP support (Session Initiation Protocol – SIP)** is an application protocol that uses a model "request-response," similar to HTTP to start calls and conferences through the network via IP protocol.

Some applications may not work with the SIP support enabled.

- **DCE-RPC TCP support**: enables the support to protocol DCE-RPC TCP.

Default value: **DCE-RPC TCP support is enabled.**

The DCE/RPC TCP is a type of RPC protocol (Remote Procedure Call), who has the objective of allowing the development of application client/server. It is used a lot in domain administration and remote management Server.

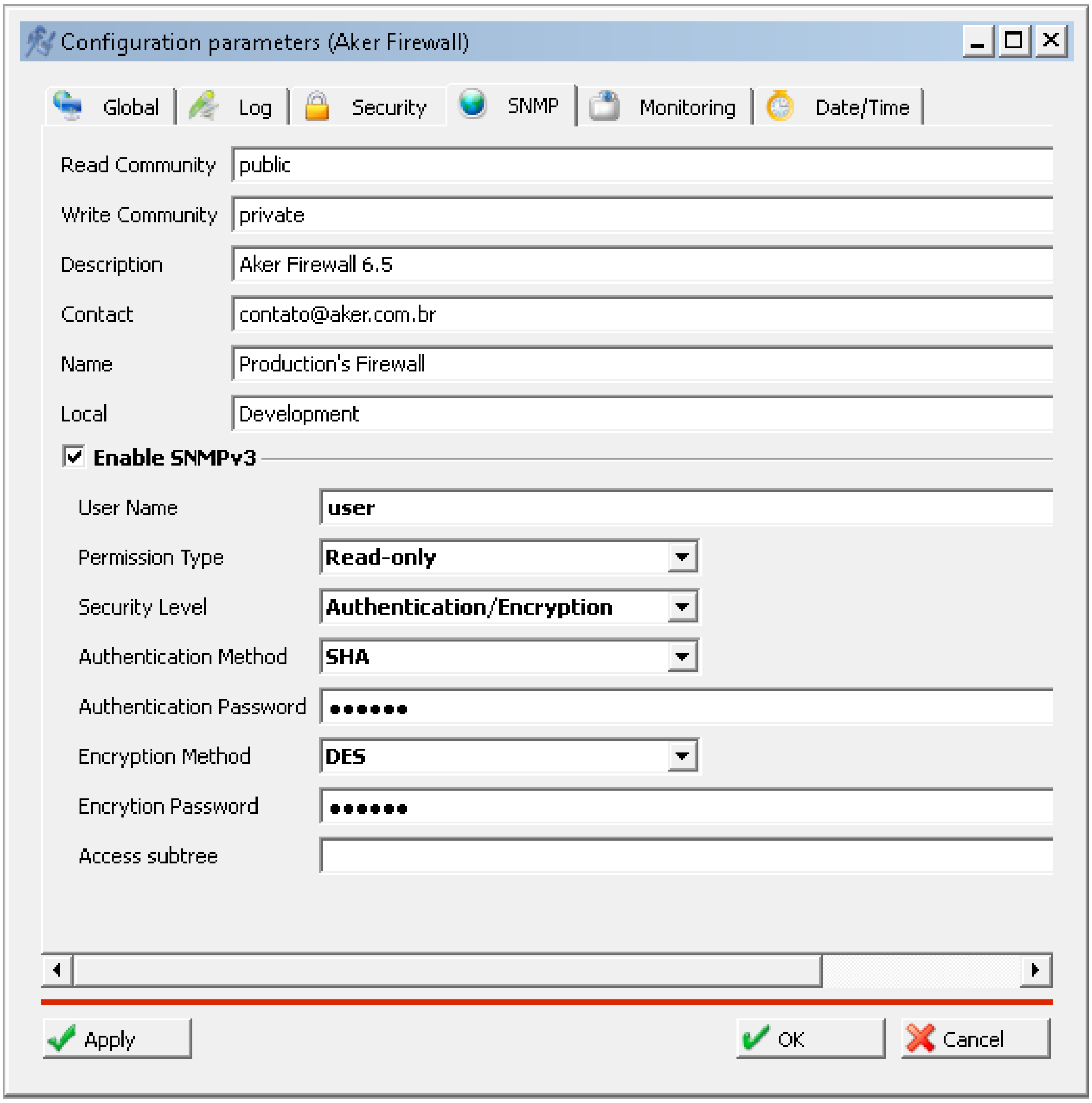
- **Keep expired rules connections:** Keep the connections even after the expiration date of the rule has been expired.

Default value: **Keep expired rules connections.**

This option allows the user to remain connected even after the end of the period defined by the connection end.

E.g. the user starts a download via FTP within the time set by rule. In case this option is checked the connection (download) will not be finished in the specified time, but after the end of the files' transfer.

SNMP tab



Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time

Read Community: public

Write Community: private

Description: Aker Firewall 6.5

Contact: contato@aker.com.br

Name: Production's Firewall

Local: Development

☑ Enable SNMPv3

User Name: user

Permission Type: Read-only

Security Level: Authentication/Encryption

Authentication Method: SHA

Authentication Password: ●●●●●●

Encryption Method: DES

Encrytion Password: ●●●●●●

Access subtree:

Apply
OK
Cancel

Image 135 – Configuration parameters: SNMP tab

- **Read Community;** This parameter indicates the community name that is authorized to read firewall data via SNMP. In case this field is in blank, no host will be authorized to change them.

Default value: ***In blank***

- **Write Community:** This parameter indicates the community name that is authorized to change firewall data via SNMP. In case this field is blank, no host will be authorized to change them.

Default value: ***In blank***

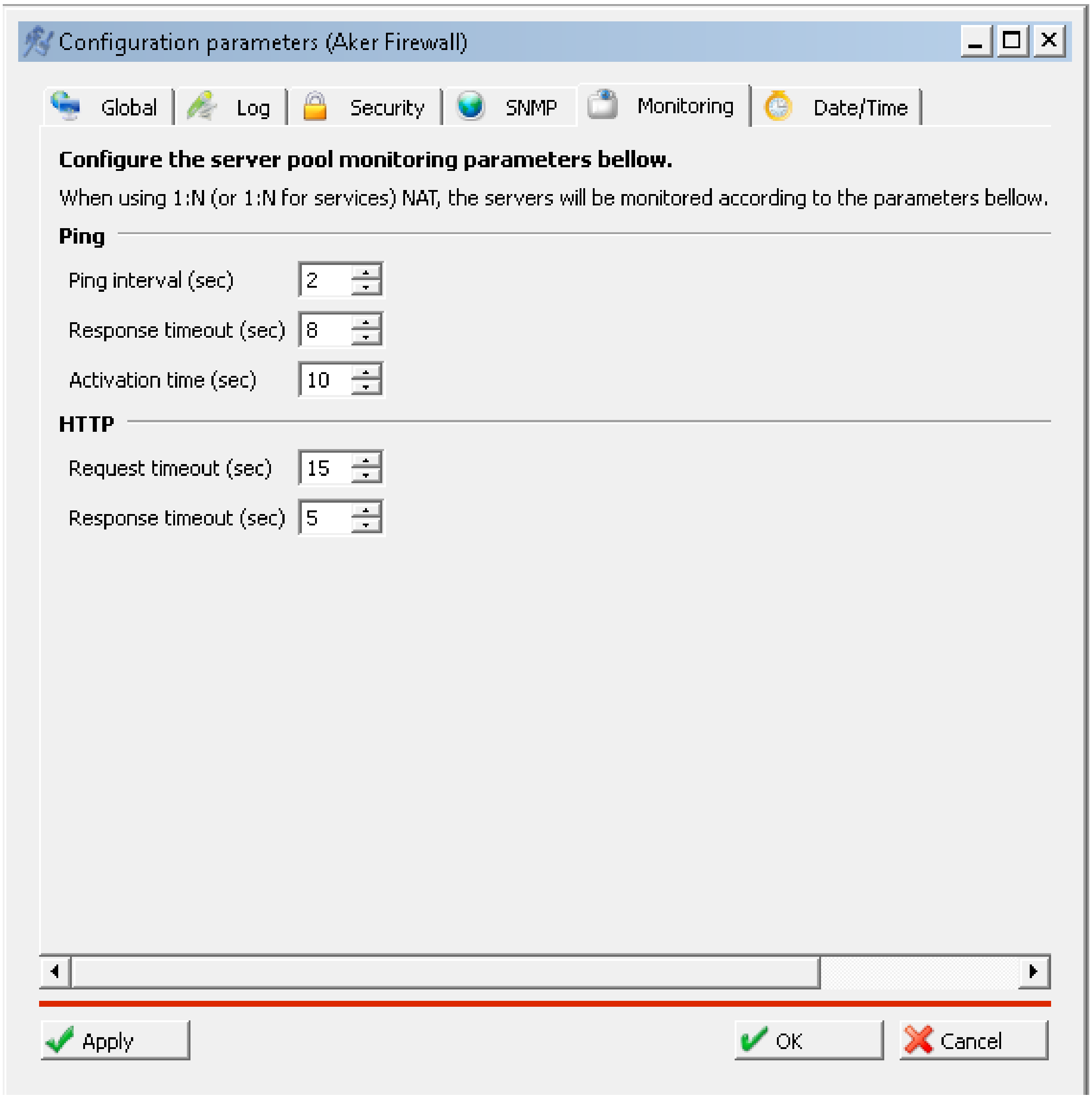
Even with a write community defined, by security reasons, only few variables will be allowed to change in the ***system group***.

- **Description:** Type of service the host provides to the user.
- **Contact:** Agreement type (e-mail, home page) that the administrator provides to user.
- **Name:** Short name of system which identify the network e.g.: DNS
- **Local:** Physical location where the host is installed.

The SNMPv3 includes three important services: authentication, privacy and access control.

- **Enable SNMPv3:** By selecting this option allows defining the type of permission of a user and in what security level user will be related to.
- **User Name:** User name that will have permission to check or modify the information.
- **Permission Type:** Allows choosing a type of permission to user.
- **Security Level:** Allows choosing a type of data security. User can choose no authentication, with authentication or authentication with encryption. In case is with authentication, the options authentication method and authentication password will be enabled. In case of choosing authentication with encryption, the options Encryption Method and Encryption password will be enabled.

Monitoring tab


Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time
Apply
OK
Cancel

Configure the server pool monitoring parameters bellow.

When using 1:N (or 1:N for services) NAT, the servers will be monitored according to the parameters bellow.

Ping

Ping interval (sec): 2

Response timeout (sec): 8

Activation time (sec): 10

HTTP

Request timeout (sec): 15

Response timeout (sec): 5

Image 136 –Configuration parameters: Monitoring tab

Using the address translation 1-N, in other words balancing channel, is possible to configure a type of monitoring to be performed by the firewall to verify if the hosts that are part of the load balancing are online. The monitoring parameters allow modifying the monitoring time intervals, in order to better adjust them in each environment.

Monitoring via ping.

These parameters configure the times used by firewall to perform the monitoring via packets *ICMP Echo Request* and *Echo Reply*. They are:

Ping Interval: This field defines in how many seconds, the ping will be sent to the monitored hosts. Its value may vary between 1 and 60 seconds

Default value: ***2* seconds**.

Response timeout: This field defines the maximum time (in seconds) that the host can remain without answer the ping packets sent by the firewall and still be considered as active.

Default value: ***8* seconds.**

Activation time: This field defines the time (in seconds) which the firewall will wait, after receiving a response packet from the previously offline host, until consider it online again. This time interval is necessary, because usually host responses to ping packets before all of its services are activated. Its value may vary between 1 and 60 seconds.

Default value: ***10* seconds**.

Monitoring via http

These parameters configure the time used by the firewall to do the monitoring via HTTP requests. They are:

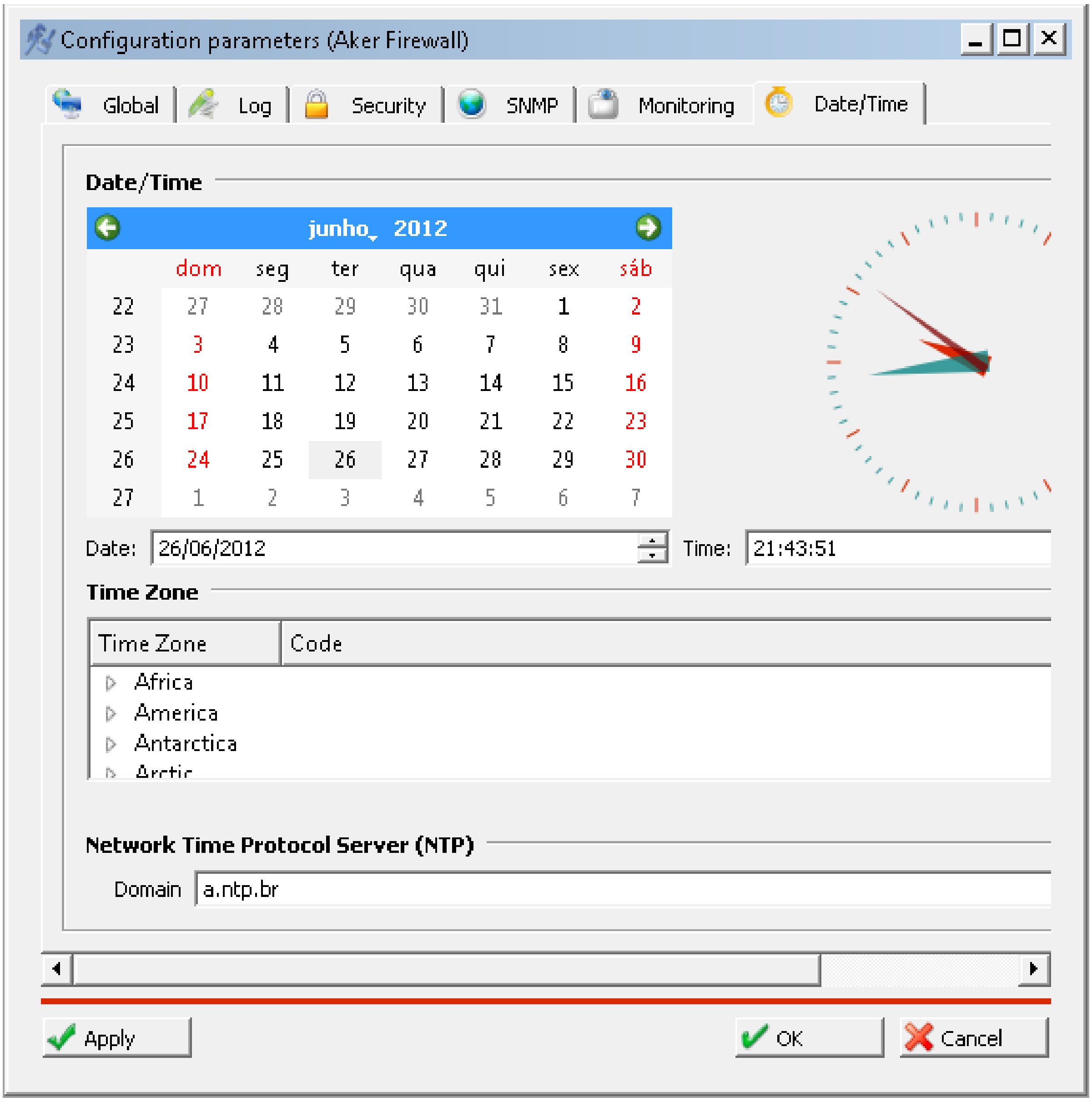
Request timeout: This field defines in how many seconds the firewall will request the specified URL by the administrator to each host being monitored. Its value may vary between 1 and 300 seconds.

Default value: ***5 seconds***.

Response timeout: This field defines the maximum time (in seconds) which the monitored host will take to answer the firewall request and still be considered active. Its value may vary between 2 and 300 seconds.

Default value: ***15* seconds**.

Date/Time tab


Configuration parameters (Aker Firewall)
Global
Log
Security
SNMP
Monitoring
Date/Time
Date/Time
junho 2012
Time Zone
Network Time Protocol Server (NTP)
Apply
OK
Cancel

	dom	seg	ter	qua	qui	sex	sáb
22	27	28	29	30	31	1	2
23	3	4	5	6	7	8	9
24	10	11	12	13	14	15	16
25	17	18	19	20	21	22	23
26	24	25	26	27	28	29	30
27	1	2	3	4	5	6	7

Date: 26/06/2012 Time: 21:43:51

Time Zone	Code
Africa	
America	
Antarctica	
Arctic	

Domain a.ntp.br

Image 137 – Configuration parameters – Date/Time

This option allows the administrator to verify and change the firewall date and time. The date and time need to be setup correctly in order to the rules' timetables and the access profiles WWW (WORLD WIDE WEB) work properly, the key change through the SKIP protocol and the system of log and events.

- **Date and Time**

This window contains two fields that show the Date/time value configured in the firewall. To change any of these values, just need to put the desired value in the corresponding field. To choose the month just need to use the navigation keys.

- **Time Zone**

Choose the Time Zone which is closer to the region where the firewall will be installed.

- The ***Apply*** button changes the date/time and it keeps the window opened.
- The ***OK*** button will close the window and save the changes.
- The ***Cancel*** will close the window without saving any changes.

- **Network Time Protocol Server (NTP)**

Defines the time sever that will be used by firewall to synchronize its internal clock. (This field just appears to the Firewall Box)

5.2. Using the text interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action)*. It also has options that are not available in the Remote Interface one of them is add up to 3 hosts capable of administrating the firewall remotely, even without a rule releasing its connection. The purpose of this feature is allows that, even if an administrator has made a wrong setup which prevents the connection, yet he will be able to administrate the firewall remotely. This parameter is called **end_remoto**.

Program location *: /aker/bin/firewall/fwpar*

Syntax*:*

fwpar *– Show/change the configuration parameter*

Usage*:*

fwpar [show | help]

fwpar External_interface <name>

fwpar [time_limit_tcp | time_limit_udp] <seconds>

fwpar [ip_directed] <yes | no>

fwpar [support_h323 | support_msn | support_sip | support_dce_rpc | keep_connect_exp] <yes | no>

fwpar [support_ftp | support_real_audio | support_rtsp] <yes | no>

fwpar [log_translation | log_syslog] <yes | no>

fwpar [permanence_log | permanence_event | permanence_stat] <days>

fwpar [serv_log_remote <name>]

fwpar [add_remote <n> <ip_add>]

fwpar [snmp] [rocommunity | rwcommunity | description | contact | name | location] [name]

show *= shows current configuration*

help *= shows this message*

external_interface *= configures external interface name (connections which came through this interface doesn't count in license)*

time_limit_tcp *= inactivity maximum time for TCP connections*
time_limit_udp *= inactivity maximum time for UDP connections*
directed_ip *= accepts directed ip*

support_ftp *= enables support to FTP protocol*

support_real_audio *= enables support to Real Audio protocol*

support_rtsp *= enables support to RTSP protocol*

support_pptp *= enables support to Microsoft(R) PPTP protocol*

support_h323 *= enables support to H.323 protocol*

support_sip *= enables support to SIP protocol*

support_dce_rpc *= enables support to DCE-RPC protocol about TCP*

keep_connect_exp *= keeps expired rules connections*

log_translation *= registers messages of address translation*

log_syslog *= sends log and events messages to syslogd*

permanence_log *= permanence time (days) log registers;*

permanence_event *= permanence time (days) events registers;*

permanence_stat *= permanence time (days) statistics;*

serv_log_remote *= remote log sever (entity name);*

end_remote *= addresses of the three remote controllers;*

rocommunity *= reads community name to SNMP*

rwcommunity *= writes community name to SNMP*

Example 1: (visualizing configurations)

# ***fwpar shows global parameters***:

```
--------------------
time_limit_tcp  : 900 seconds

time_limit_udp  : 180 seconds

external_interface: lnc0
```

Security parameters:

----
directed_ip : no

support_ftp : yes

support_real_audio: yes

support_rtsp : yes

end_remote : 1) 10.0.0.1 2) 10.0.0.2 3)10.0.0.3

Log configuration parameters :

----
log_translation : no

log_syslog : no

permanence_log : 7 days

permanence_event : 7 days

permanence_stat : 7 days

SNMP Configuration parameters:

Example 2: (enable directed IP packet)

```
#/aker/bin/firewall/fwpar directed_ip yes
```

Example 3: (configuring the SNMP read community name)

```
#/aker/bin/firewall/fwpar rocommunity public
```

Example 4: (deleting write community name SNMP)

```
#/aker/bin/firewall/fwpar rwcommunity
```

Registering Entities

6. Registering Entities

This chapter will show what is and how to register entities in Aker Firewall.

6.1. Planning installation

What are the entities for?

Entities are representations of real world objects to Aker Firewall. Through them, the hosts, network, services to be provided, among others that can be represented.

The main advantage of the entities use to represent real objects is that from the moment they are defined in the firewall, they can be referenced like if they were the objects itself, providing a greater facility to configure and operate. All the made changes in an entity will be automatically widespread to all locations where it is referenced.

It can be set, for instance a host called **WWW (WORLD WIDE WEB) SERVER**, with the IP address **10.0.0.1**. From this moment, is not necessary to worry about this IP address. In any point where is necessary to refer about this host, the reference will be made by the name. Later if its IP address need to be changed, simply change the entity definition that the system will automatically program this change to all of its references.

Defining entities

Before explaining how to register entities in Aker Firewall is required a brief explanation of the types of entities and what characterizes each one of them.

There are 9 different types of entities in Aker Firewall: IPv6 hosts, hosts networks, IPV6 networks, sets, IPV6 sets, services and authenticators and interfaces.

The entities host type and network, as the name implies, represent individual hosts and network. *Entities of type SET* represent a collection of hosts and networks, in any number. *Entities of type SERVICE* represents a service to be made available through a protocol that runs on top of the IP. *Entities of type AUTHENTICATOR* represent a special type of host that can be used to perform user authentication and *Entities of type INTERFACE* represent a network interface of the firewall.

By definition, the protocol requires each host to have a different address. Usually these addresses are represented as byte-by-byte, for instance, 172.16.17.3. In this way can be characterized only a host in any IP network, including the internet, just with its address.

To define a network should use a mask beyond the IP address. The mask is used to define which bits of the IP address will be used to represent the network (bit with value 1) which will be used to represent the hosts within the network (bit with 0 value). This way, to represent the network that hosts can assume the IP addresses 192.168.0.254 to 192.168.0.254, shall put the network with value 192.168.0.0 and with mask 255.255.255.0. This last byte is used to represent the host.

To verify if the host belongs to a specific network, just need to make a logical AND of the network mask, with the desired address and comparing with the Logical AND of the network address with its mask. If they are the same, the host belongs to the network, and if they are different they do not belong. Check the examples below:

Suppose we want to check if the host 10.1.1.2 belongs to network 10.1.0.0, mask 255.255.0.0. We have:

10.1.0.0 ***/*** 255.255.0.0 = 10.1.0.0 (To the network)

10.1.1.2 ***/*** 255.255.0.0 = 10.1.0.0 (To the address)

Then we have two same addresses after the mask applying, so the host 10.1.1.2 belongs to network 10.1.0.0.

Now suppose we want to know if the host 172.16.17.4 belongs to network 172.17.0.0, mask 255.255.0.0. We have:

172.17.0.0 **E** 255.255.0.0 = 172.17.0.0 (To the network)

172.16.17.4 **E** 255.255.0.0 = 172.16.0.0 (To the address)

As the final addresses are different, the host 172.16.17.4 does not belong to network 172.17.0.0.

In case it is necessary to set a network where any host is considered part of it (or to specify any Internet host) you shall put the IP addresses of this network the value 0.0.0.0 and as the value. This is quite useful when is needed to provide public services, where all the Internet hosts will have access.

Every time there is a communication between two hosts, using the IP protocol, are involved not only the source and destination addresses, but also a higher-level protocol (transport level) and some other data that identify the communication. In case the TCP and UDP protocols (which are the two most used), a communication is identified by two numbers: The **Source port** and the **Destination port.**

The destination port is a fixed number that is associated usually to a single service. This way, The Telnet service is associated with the TCP protocol on port 23, the FTP service with the TCP protocol on port 21 and the SNMP service with the UDP protocol on port 161, for instance.

The source port is a sequential number chosen by the client so that there is more than one active session of the same service at any moment. So, a complete communication in the TCP and UDP protocol can be represented as it follows:

10.0.0.1	1024	10.4.1.2	23	TCP
Source address	Source port	Destination address	Destination port	Protocol

For a firewall, the source port is not important, since it is random. Due to it when it defines a service, it takes into consideration only the Destination port.

Beside the TCP and UDP protocol there is another important protocol: The ICMP. This protocol is used by the IP itself to send control messages, informing about errors and test the network connectivity.

The ICMP protocol does not use the ports concept. It uses a number that vary from 0 to 255 to indicate a **Service Type**. As the service type characterizes a service between two hosts only, it can be used as if it were the protocol Destination port, (TCP and UDP) when needs to define a service.

Finally, there are other protocols that can run on the IP protocol and that are not TCP, UDP, or ICMP. Each one of those protocols has their own ways to define a communication and none of them is used by a large number of hosts. Yet, the Aker Firewall opted to add support to make possible to the administrator control which of these protocols may or may not pass through the firewall.

To understand how it is done, just need to know that each protocol has a single number that identify to the IP protocol. This number varies from 0 to 255. This way, we can define services to other protocols using the number of protocol as identification of service.

What is Quality of Service (QoS)?

The quality of service can be understood in two ways: from the application or network point of view

To an application offers its services with quality, it has to meet user expectations in relation to the response time and the quality of service which is being provided. For instance, in case a video application, fidelity sound and/or image without noise or freezing.

Network quality of service depends on the needs of the application, i.e. what it requests from the network in order to work well and meet the clients' need. These requirements are translated into network indicators parameters such as the maximum delay suffered by the application traffic, between ***the Source and the Destination computer.***

The Aker Firewall implements a mechanism which is possible to set maximum bandwidth traffic for certain applications. Through its use certain application that traditionally consume too much bandwidth, can have their use controlled. The Channel type entities are used for this purpose and will be explained below.

6.2. Registering entities using the Remote Interface

To gain access to registering entities window, follow the steps bellow:

- Click on the *firewall configuration* menu from the firewall you wish to administrate.
- Select *Entities* (the window ***Entity*** will be displayed, below the firewall configuration menu window)

The Entities registration window

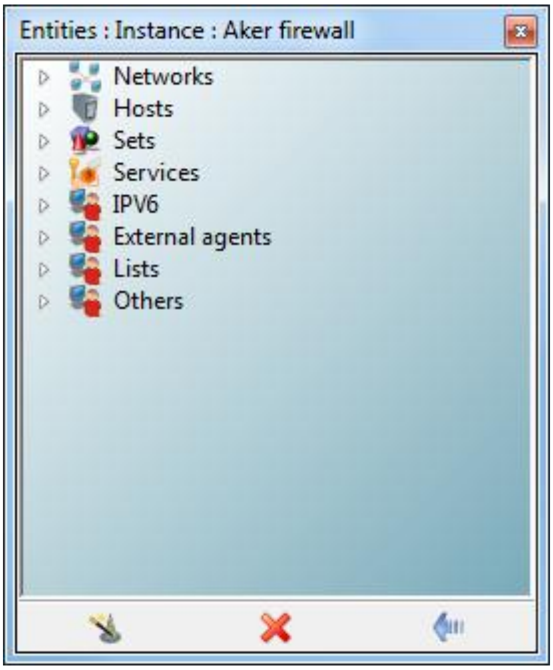
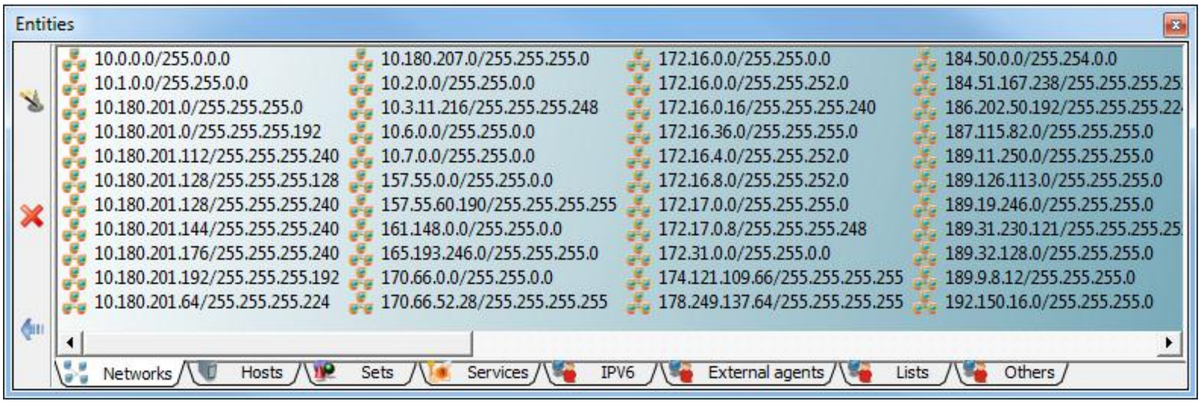

Entities : Instance : Aker firewall
Networks
Hosts
Sets
Services
IPV6
External agents
Lists
Others

Image 138 – Entities window (Aker Firewall)

You can also access the Entities window hitting the F5 button:

F5 button

Image 139 – F5 button on your keyboard.



10.0.0.0/255.0.0.0
10.1.0.0/255.255.0.0
10.180.201.0/255.255.255.0
10.180.201.0/255.255.255.192
10.180.201.112/255.255.255.240
10.180.201.128/255.255.255.128
10.180.201.128/255.255.255.240
10.180.201.144/255.255.255.240
10.180.201.176/255.255.255.240
10.180.201.192/255.255.255.192
10.180.201.64/255.255.255.224
10.180.207.0/255.255.255.0
10.2.0.0/255.255.0.0
10.3.11.216/255.255.255.248
10.6.0.0/255.255.0.0
10.7.0.0/255.255.0.0
157.55.0.0/255.255.0.0
157.55.60.190/255.255.255.255
161.148.0.0/255.255.0.0
165.193.246.0/255.255.255.0
170.66.0.0/255.255.0.0
170.66.52.28/255.255.255.255
172.16.0.0/255.255.0.0
172.16.0.0/255.255.252.0
172.16.0.16/255.255.255.240
172.16.36.0/255.255.255.0
172.16.4.0/255.255.252.0
172.16.8.0/255.255.252.0
172.17.0.0/255.255.255.0
172.17.0.8/255.255.255.248
172.31.0.0/255.255.0.0
174.121.109.66/255.255.255.255
178.249.137.64/255.255.255.255
184.50.0.0/255.254.0.0
184.51.167.238/255.255.255.25
186.202.50.192/255.255.255.22
187.115.82.0/255.255.255.0
189.11.250.0/255.255.255.0
189.126.113.0/255.255.255.0
189.19.246.0/255.255.255.0
189.31.230.121/255.255.255.25
189.32.128.0/255.255.255.0
189.9.8.12/255.255.255.0
192.150.16.0/255.255.255.0

Image 140 – Entities: Aker Firewall Instance.

The entities registration window is where all of Aker Firewall entities are registered, independent of its type. This window is constantly being used practically in all other firewall settings, normally is displayed in horizontal, below each window with configuration menus for each firewall.

Hint: There will be a single window for all open firewalls. The window will remain the same, only the content that is referent to the selected firewall will be changed. The most used types of entities are the ones presented in the tab. The Less used entities will appear in the menu.

Hint: It is possible to position the entities window as if it were a common window, just clicking on its title bar and drag to the desired position.

Hint: To create a new entity, in case the created entities list is full, you have to click on the tab that is located at the bottom of the window.

In this window there are eight icons drawn, in a tree-shaped that represents the eight types of entities that can be created.

Hint: To visualize the created entities just click on the '+' and the entities will be listed just below the logo, or just click on the corresponding to the entity that you wish to visualize.

To register a new entity, proceed as follows:

1. Click once on the corresponding icon of the entity type you wish to create, right-click and select the option “***Insert”*** in the pop-up menu.

   Or

2. Click on the corresponding icon of the entity type you wish to create and press the “***Insert”*** key.

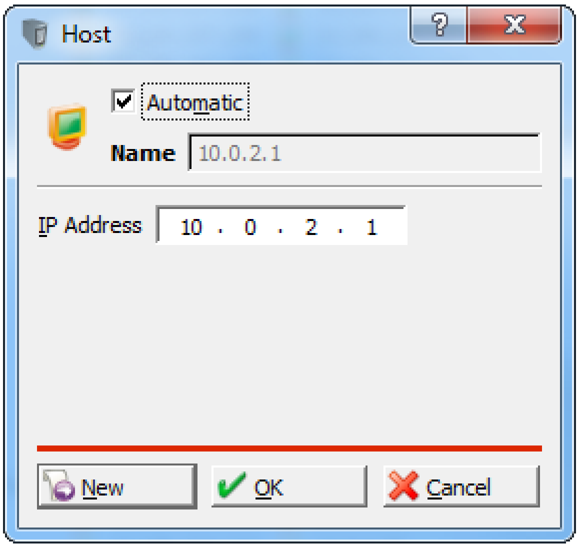
To edit or delete an entity, proceed as follows:

1. Select the entity to be edited or deleted (if necessary, expands the corresponding entity type list)
2. Right-click and select the option ***Edit*** or ***Delete***, respectively, from the pop-up menu that appears;
3. Click on the icon corresponding to the entity type you wish to create and press the **Delete** key.

In case the ***Edit*** or ***Add*** option, an entities parameter edition window will be displayed and it shall be edited and added. This window will be different for each possible type of entities.

The icon , located at the bottom of the window, it fires the Entities Registration Wizard that will be described at the end of this chapter.

Including / editing host



☑ Automatic
Name 10.0.2.1
IP Address 10 . 0 . 2 . 1

Image 141 – Registering entities: Host type.

In order to register an *entity of type host*, the following fields shall be filled in:

Name: is the name which the host will always be referenced by your firewall. You can also specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

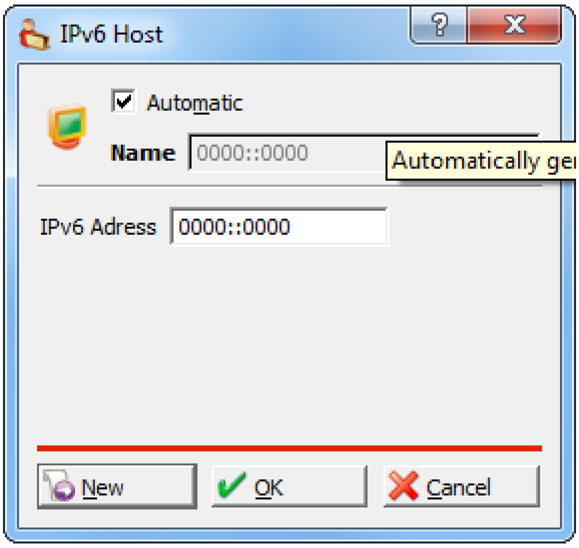
Icon: icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click the ***OK*** button**.** In case you do not want to change it after see the list, just click on the ***Cancel*** button.

IP Address: Is the IP address of the host that will be created.

After all fields are filled in, click on the ***OK*** button to perform the addition or change of the host. To cancel the additions or changes click on the ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of hosts.

Including / editing IPv6 host



☑ Automatic

Name 0000::0000 Automatically ge

IPv6 Adress 0000::0000

Image 142 – Registering entities IPv6 host type

In order to register an *entity of type* ***IPv6*** *host* the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click the ***OK*** button**.** In case you do not want to change it after see the list, just click the ***Cancel*** button.

IP Address: Is the IP address of the host that will be created.

After all fields are filled in, click on the ***OK*** button to perform the addition or change of the host. To cancel the additions our changes click on ***Cancel***.

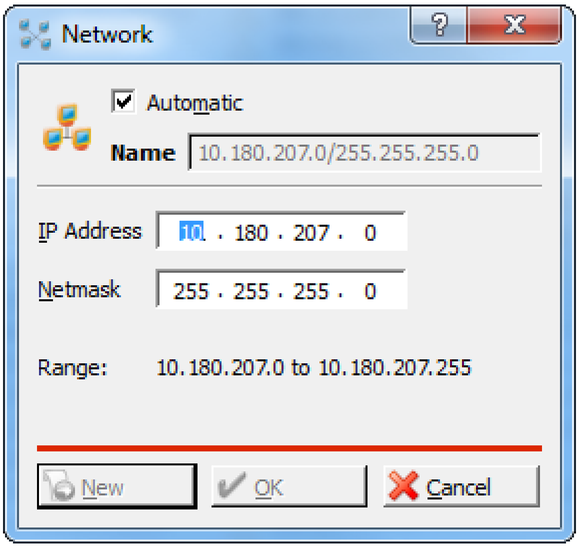
To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of hosts.

.

The expansion of 32-bits of IPv4 address to 128-bits in the IPV6 is one of the most important features of the new protocol. It is a huge address space, with a hard number to be displayed, because there are thousands of billons of addresses. IPv6 ends up with the address classes and provides a simpler method of self-configuration.

The most common notation that the IPv6 address is represented is x:x:x:x:x:x:x:x. where the "x" hexadecimal numbers, so the address is divided in eight parts of 16 bits as in the following example : **1080:0:0:0:8:800:200C:417A**

Including / editing networks



☑ Automatic

Name: 10.180.207.0/255.255.255.0

IP Address: 10 . 180 . 207 . 0

Netmask: 255 . 255 . 255 . 0

Range: 10.180.207.0 to 10.180.207.255

Image 143 – Networks adding and editing

In order to register an entity of type network, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

IP Address: Is the IP address of the host that will be created.

.

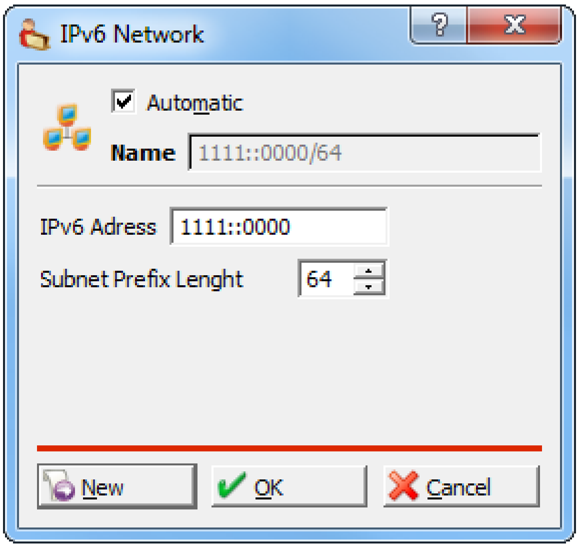
Network Mask: Defines which IP address bits will be used to represent the network (bits value 1) and which will be used to represent the host within the network (bits value 0)

Range: This field shows the IP address range that belongs to the network and performs a critique when the mask is being registered, i.e. it does not allow the registration of wrong masks.

After all the fields are filled in, click on **OK** to make the inclusion or change the network. To cancel a made change or an inclusion, click on **Cancel**.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of network.

Including / editing IPv6 Network



☑ Automatic

Name 1111::0000/64

IPv6 Adress 1111::0000

Subnet Prefix Lenght 64

Image 144 – Adding and editing IPv6 Network.

In order to register an entity of type *IPv6 network* the following field shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

IP Address: Is the IP address of the host that will be created.

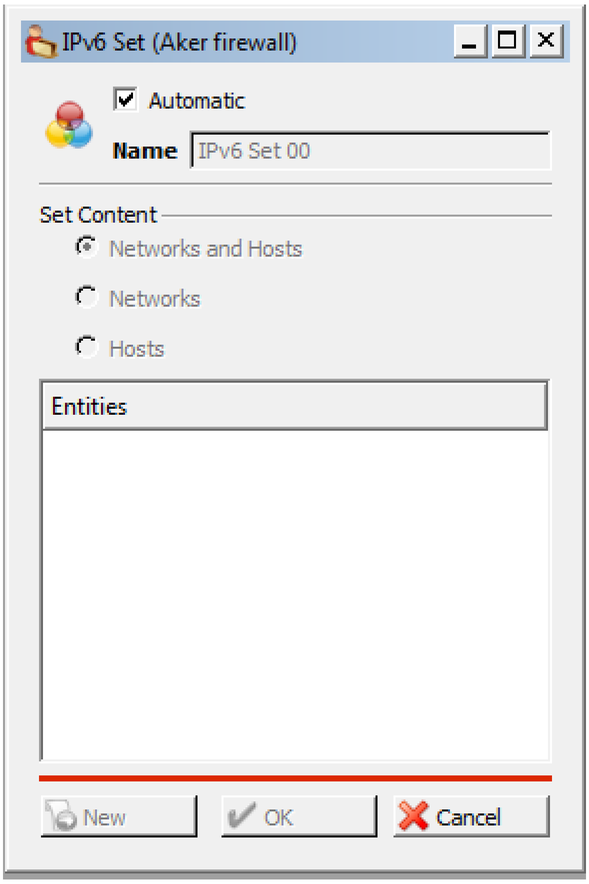
.

Subnet Prefix Length: Defines which IP address bits will be used to represent the network.

After all the fields are filled in, click **OK** to make the inclusion or change the network. To cancel a made change or an inclusion, click **Cancel**.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of network.

Including / editing Sets



☑ Automatic

Name IPv6 Set 00

Set Content

● Networks and Hosts

○ Networks

○ Hosts

Image – 145 Adding and editing IPv6 Set.

In order to register an *entity IPv6 set*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

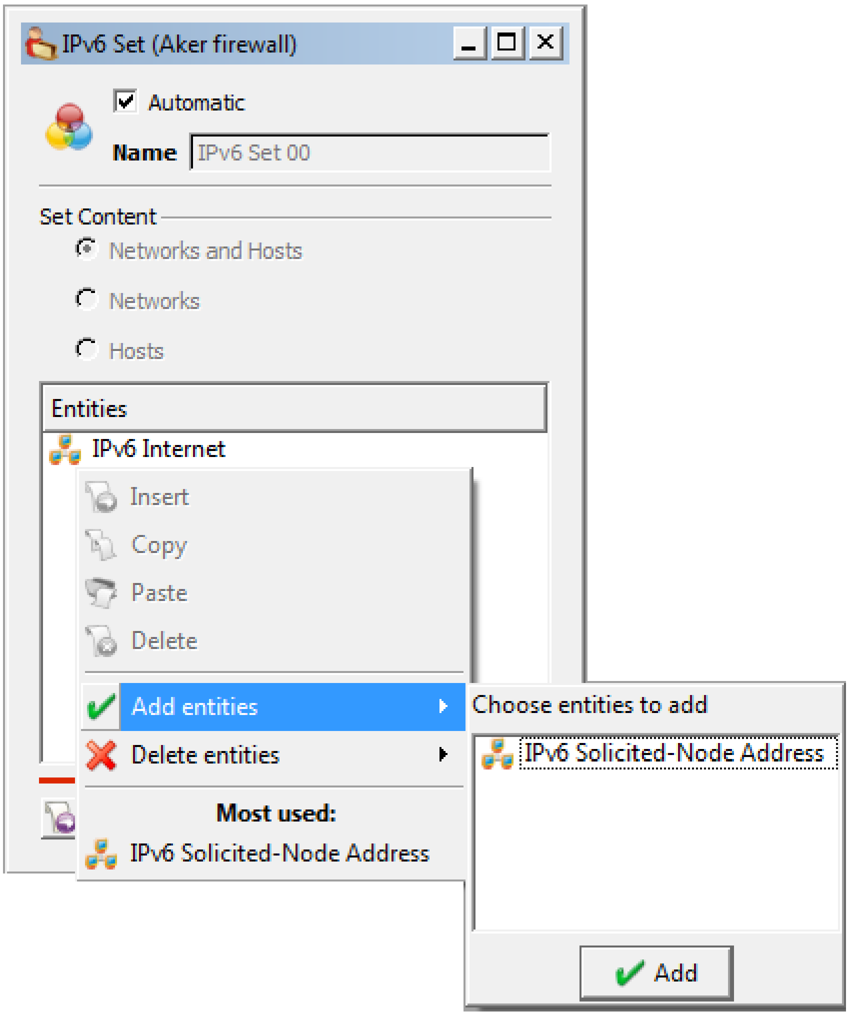
Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

After fill in the name and choose the icon for the set, you shall define which hosts and network will be part of it. Below are the steps that should be followed.

1. Right-click in the blank area and select the option **Add entities (** the entity can be added by double-clicking on it or clicking once and just **Add** below)

2. Click on the entity that you wish to include, with this should drag it and drop it inside the Set entity window.


IPv6 Set (Aker firewall)
Set Content
Entities
IPv6 Internet
Insert
Copy
Paste
Delete
Add entities
Delete entities
Most used:
IPv6 Solicited-Node Address
Choose entities to add
IPv6 Solicited-Node Address
Add

☑ Automatic

Name IPv6 Set 00

● Networks and Hosts
○ Networks
○ Hosts

Image 146 – Adding the entities.

In order to remove a network or host form a set, proceed as follows:

1. Right-click on the entity to be removed and select the option ***Delete***,

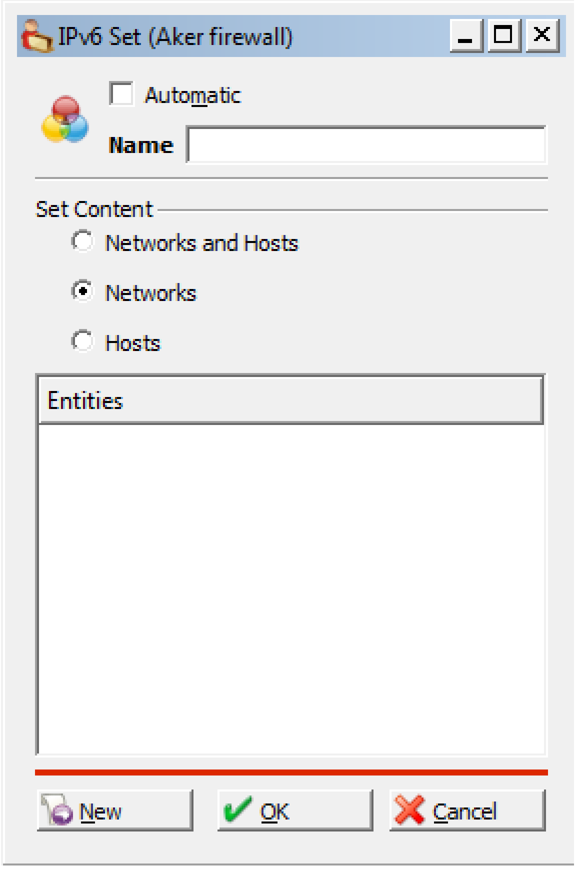
Or

2. Click on the host or network to be removed a press ***Delete*** on the keyboard.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, you shall click on ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, press ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of sets.

Editing IPv6 sets


IPv6 Set (Aker firewall)

☐ Automatic

Name

Set Content

○ Networks and Hosts

● Networks

○ Hosts

Image 147 – IPv6 set editing.

In order to register an entity of type *IPv6 set*, the following fields shall be filled in:

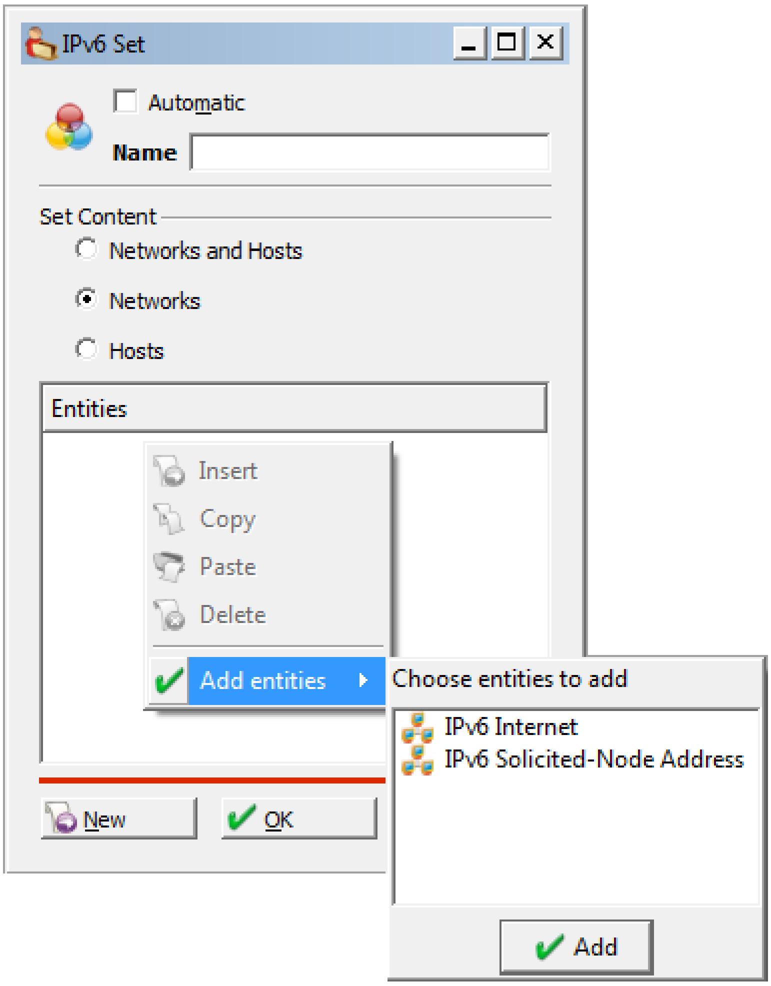
Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

After fill in the name and choose the icon for the set, shall define which hosts and network will be part of it. Below are the steps that should be followed.

1. Right-click in the blank field a select the option ***Add entities*** (the entity can be added by double-click or clicking once and just below on ***Add***). Or
2. Click on the entity that you wish to add, and drag it and drop it inside the entities window in the set.



IPv6 Set

☐ Automatic

Name

Set Content

○ Networks and Hosts

● Networks

○ Hosts

Entities
Insert
Copy
Paste
Delete
Add entities
Choose entities to add
IPv6 Internet
IPv6 Solicited-Node Address
Add
New
OK

Image 148 – IPv6 set editing (entities to be added).

In order to remove the network or a host set, proceed as follows:

1. Right-click on the entity to be removed and select the option ***Delete.***

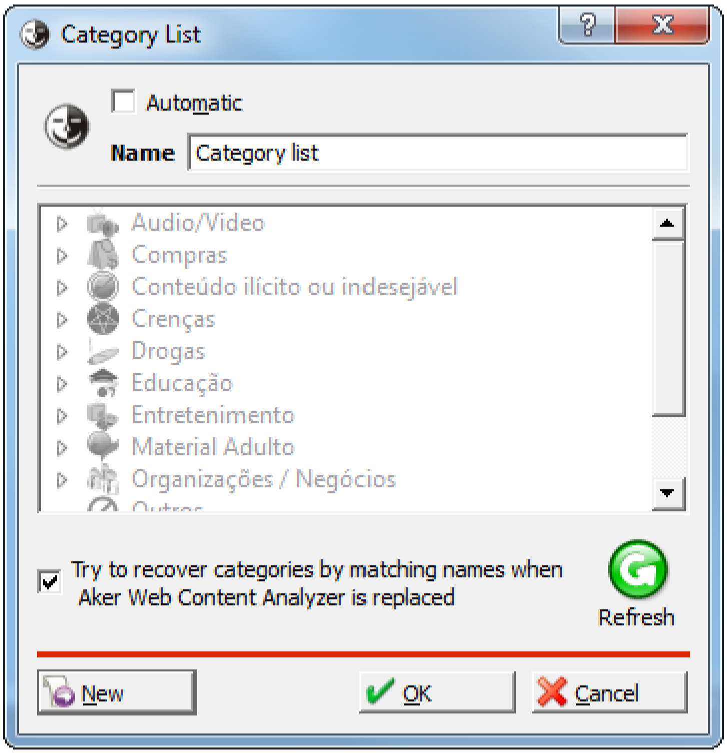
   Or

2. Click on the host or network to be removed and press the ***Delete*** key.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, you shall click on ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, press ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number of sets.

Adding / Editing Category List


Category List
? X
☐ Automatic
Audio/Video
Compras
Conteúdo ilícito ou indesejável
Crenças
Drogas
Educação
Entretenimento
Material Adulto
Organizações / Negócios
Outros
Refresh
New
OK
Cancel

Name Category list

☑ Try to recover categories by matching names when Aker Web Content Analyzer is replaced

Image 149 Category List adding and editing.

In order to define a category list proceed as follows:

Select the ***Automatic*** option, in case wish to assign a default name to the list.

Fill in the name field, where a specific name can be defined to the category list.

The ***Refresh*** button allows you to browse the categories in the firewall in case there was any update.

By selecting the option Try to recover categories by matching names, when Aker Web Content Analyzer is replaced, allows to identify the categories through the names that have been registered, because when the context analyzer is changed many categories can be lost.

Adding/ Editing Search Pattern List

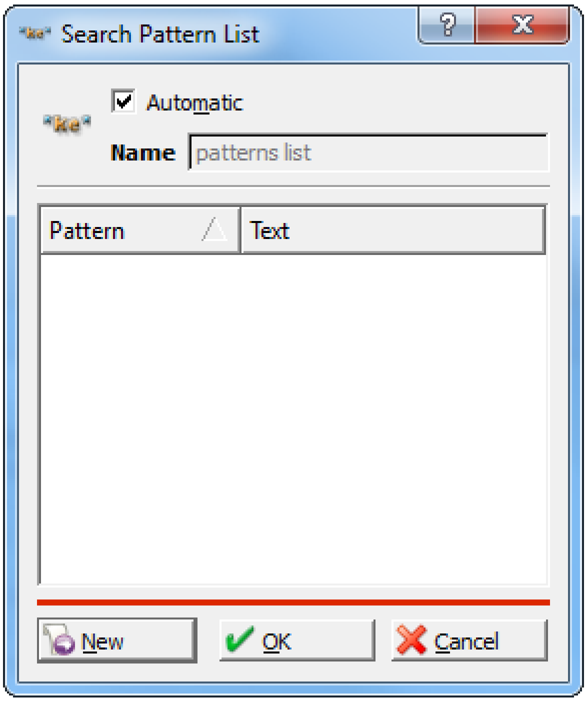

Search Pattern List
☑ Automatic
Name
patterns list
Pattern
Text
New
OK
Cancel

Image 150 – Search Pattern List adding and editing.

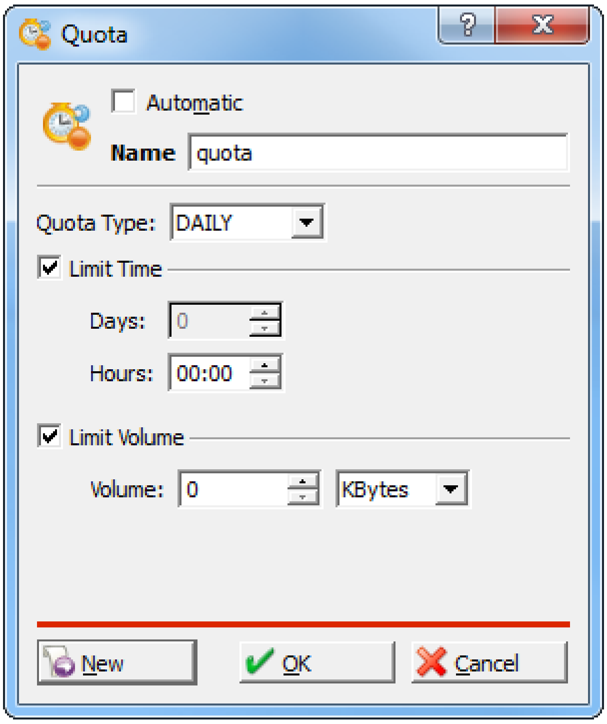
In order to define a search pattern, proceed as follows:

Select the ***Automatic*** option, in case you wish to assign a default name to the search

Fill in the name field, where a specific name for the search can be set.

The fields ***Pattern*** and ***Text***, allows defining which will be the String or the parameters that will be searched in the accessed URL and what operation to be performed.

Adding / Editing Quota



☐ Automatic
Name: quota
Quota Type: DAILY
☑ Limit Time
Days: 0
Hours: 00:00
☑ Limit Volume
Volume: 0 KBytes

Image 151 – Quota adding and editing.

This Window allows defining many types of access quotes from user to network

In order to create a quote, you can select the ***Automatic*** option to assign a default name to the quote type to be set or then fill in the field name, where you can assign a specific name to the quota list.

The option ***Quota Type*** allows choosing if the chosen quota will be assigned daily, weekly or monthly. By checking which quota type you want, you can assign to it a ***Limit Time*** and a ***Limit volume***.

The check time can be defined in days and/or hours. For example, daily only 4 hours will be released for Internet access, or weekly 3 days or even weekly 7 days.

Note 1: The timing works as follows: when the user access the page, has 31 seconds, if the user access another page, starts the 31 seconds countdown again, but it does not stop counting.

Note 2: For the quota consumption, works as follows: In the MSN, for each conversation window, the time is counted separately, but on the web if you have accessed 10 pages, they will be counted as one.

Adding / Editing External agents

External agents are used for the definition of complementary programs to Aker Firewall. They are responsible for specific functions that can be running in different hosts. When there is a need to do specific task by one of the external agents, or vice versa, the firewall will communicate with them and will request its execution.

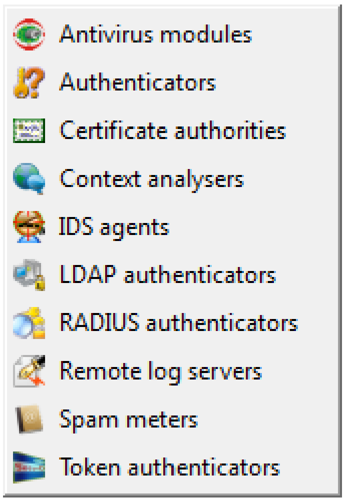

Antivirus modules
Authenticators
Certificate authorities
Context analysers
IDS agents
LDAP authenticators
RADIUS authenticators
Remote log servers
Spam meters
Token authenticators

Image 152 – External agents adding and editing.

There are 10 different types of external agents, each one of them is responsible for a type of task.

- **Authenticators**

  The agents' authentication is used to do the user authentication in the firewall using Username/Password for databases of many operating systems (Windows NT, Linux, etc.).

- **Certificate authorities**

  Certificate authorities are used to do the user authentication through the PKI, using the Smart Cards and to the firewall authentication using IPSEC encryption.

- **Token authenticators**

  The token are used to do the user authentication in the firewall using SecurID$^{(R)}$, Alladin and others.

- **IDS agents**

  The IDS agents (Intrusion Detection Systems) are systems which are monitoring the network in real-time looking for known patterns of attacks or abuse. When it detects one of these threats, it can add a firewall rule to block the attacker access immediately.

- **Antivirus modules**

  The anti-virus modules (agents) are used by proxy SMTP, POP3 and Web Filter to do the checking and virus disinfection transparently in emails and in the FTP and HTTP downloads.

- **Context analyzers**

  The context analyzers are used by the Web Filter to control the access to URLs, based in many preconfigured categories.

- **Remote log servers**

  The remote log server is used by the firewall to send the log to the storage in a remote host.

- **Radius authenticators**

  The Radius authenticators are used to do the user authentication in the firewall through a Radius base.

- **LDAP authenticators**

  The LDAP authenticators allow the firewall to authenticate the user using the LDAP base compatible with the X.500 protocol.

- **Spam Meters**

  The spam meters are used by the firewall to classify e-mails and define each of them are considered SPAM.

It is possible to install several external agents in the same host, as long the agents are alike.

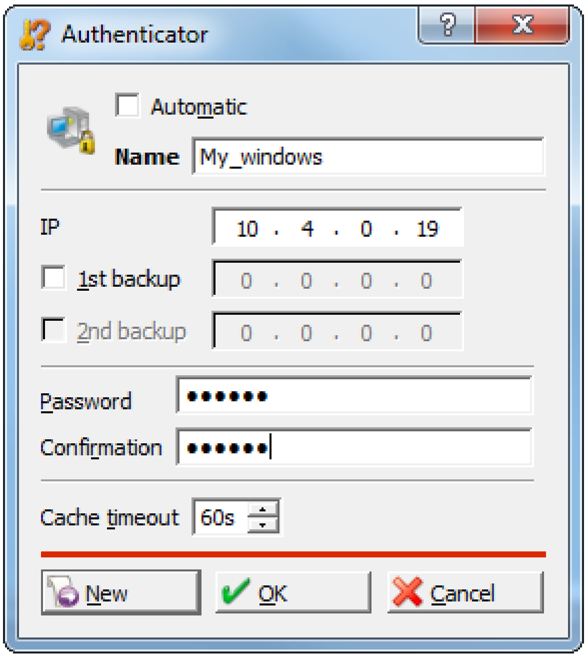
In order to register an external agent, shall select its type, opening the External Agents directory. Regardless of its sub-type, all external agents have the following fields (all other fields will be modified according to the agent type to be registered)

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

- In order to register an external agent type Authenticator or Authenticator Token, is necessary to fill in the following fields:



☐ Automatic
Name: My_windows
IP: 10 . 4 . 0 . 19
☐ 1st backup: 0 . 0 . 0 . 0
☐ 2nd backup: 0 . 0 . 0 . 0
Password: ••••••
Confirmation: ••••••
Cache timeout: 60s

Image 153 – External agent registration *Authenticator or Authenticator token* type.

IP: It is the host IP address where the agent is running.

1st Backup and **2nd Backup** : This fields allow specifying up to two addresses of other hosts that are running the agent and that will be used as backup in case the main host goes down.

The main host and the backup ones shall share the same user base, (PDCs and BDCs) in case the networks Windows or several Unix hosts are using NIS.

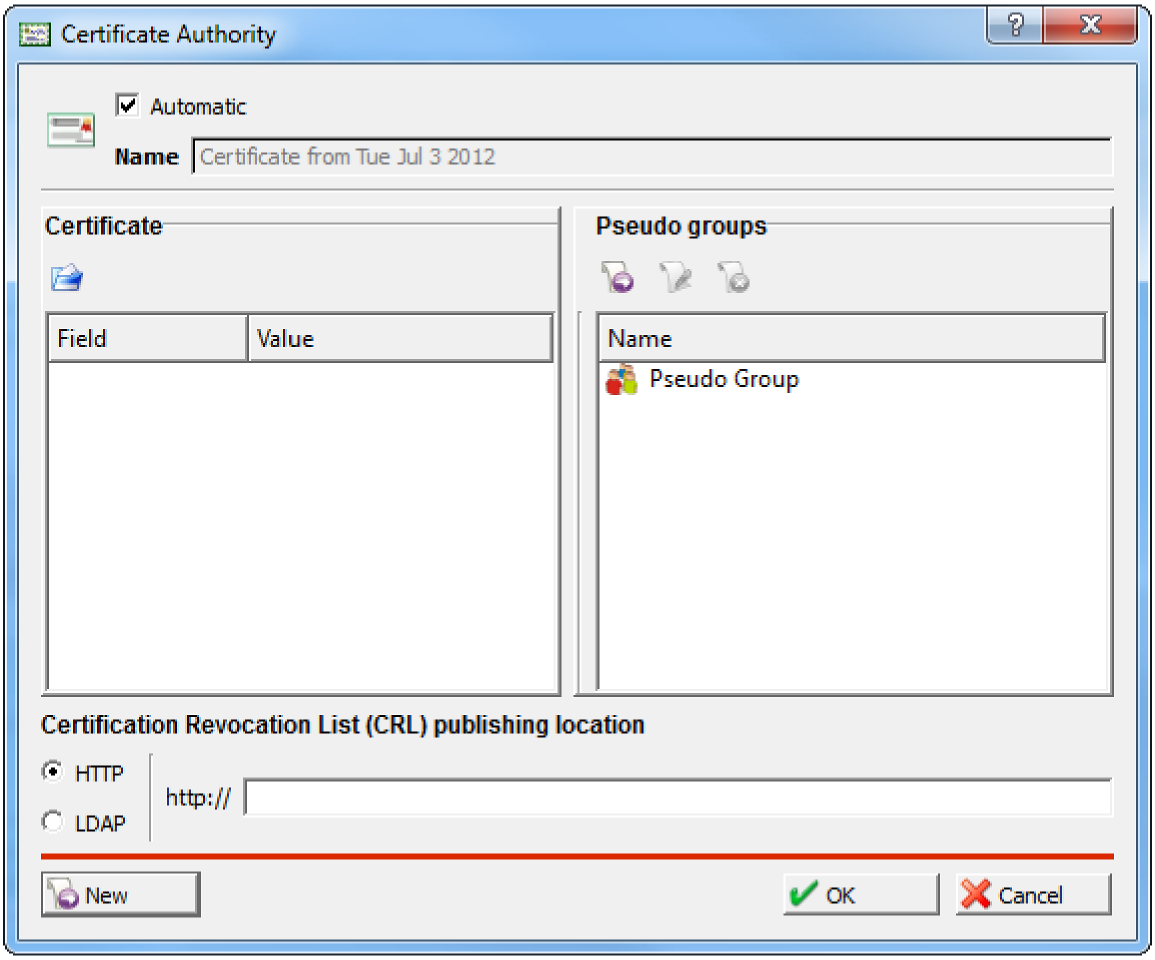
Password: Is a password used to generate the encryption and authentication Keys used in the communication with the agent. This password shall be same as the one configured in the agent. For more information, see the chapter titled: **Working with proxies.**

Confirmation: This field is used only to verify if the password was entered correctly. It shall be entered exactly as in the password field.

Cache timeout: Every time a successful authentication is made the firewall keeps in its memory the received data form the user and the agent. In the following authentications, the firewall has all the necessary data and does not need to consult the agent. This allows a great performance gain.

This parameter allows setting the time in seconds that the firewall has to keep the authentication information in memory. For more information, see the chapter titled: **Working with the proxies.**

In order to register an external agent Certificate authority, the following fields shall be filled in:


Certificate Authority
Certificate
Field
Value
Pseudo groups
Name
Pseudo Group
Certification Revocation List (CRL) publishing location
New
OK
Cancel

☑ Automatic

Name: Certificate from Tue Jul 3 2012

● HTTP
○ LDAP

http://

Image 154 – External agent registration *Certificate Authority* type.

Certification Revocation List (CRL) publishing location: is the URL which the certificate revocation list from CA (CRL) will be downloaded. This URL shall be of the HTTP protocol and shall be specified without the http://.

The ***Import the root certificate*** button allows loading the CA root in the firewall. When clicked, the interface will open a window to specify the file name with the certificate to be imported.

Is necessary to import the root certificate for each certification authority created, otherwise will not be possible to authenticate user through it.

The **Pseudo-groups** allows defining a group for the users that authenticate through the certification authority, in the same way as defines groups in an operating system. This way, it is possible to create a pseudo-group that represents all the users in a particular company, department, city, etc. After being created the pseudo-groups can be assigned to the access profiles, in the same manner as it is done with the authenticators or the token authenticators.

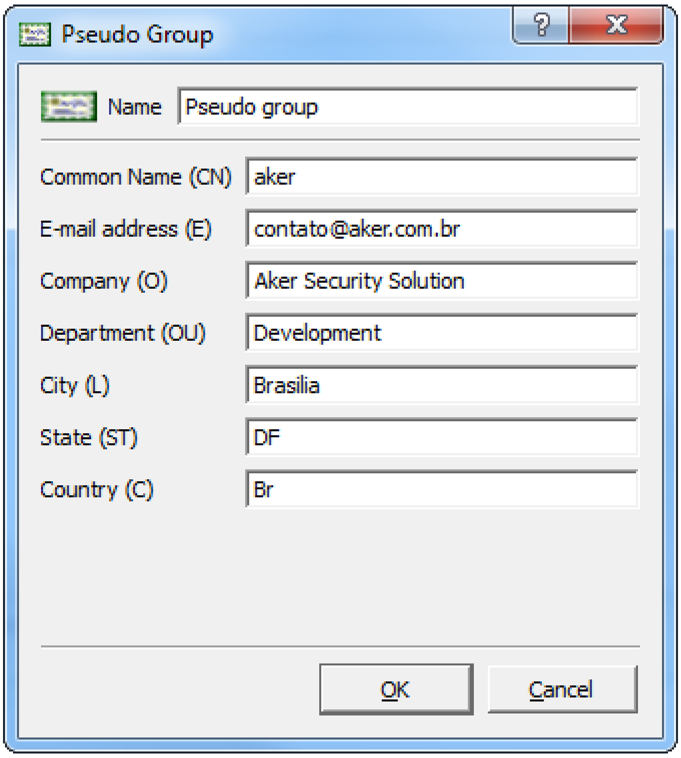
Right-click and we can select one of the following options:

Insert: This option allows adding a new pseudo-group

Delete: This option removes from the list the selected pseudo-group

Edit: This option opens an editing window for the selected pseudo-group

When clicking **Insert** or **Edit**, the following window will be displayed:



Name: Pseudo group

Common Name (CN): aker

E-mail address (E): contato@aker.com.br

Company (O): Aker Security Solution

Department (OU): Development

City (L): Brasilia

State (ST): DF

Country (C): Br

Image 155 – Pseudo Group definition to users that authenticate themselves through the certification authority.

Name: Required field which indicates the Pseudo-group name that will be referenced by the firewall. The remaining field represents data that will be compared with the data in the X.509 certificate for each authenticated user. If a particular field is in blank then any value will be accept in the certificate corresponding field, otherwise only the certificates that has its field same as the informed value would be considered as part of the group.

Common Name (CO): Certified person name

Email: email address

Company: Company name

Department: Department within the company

City: City which is located the company

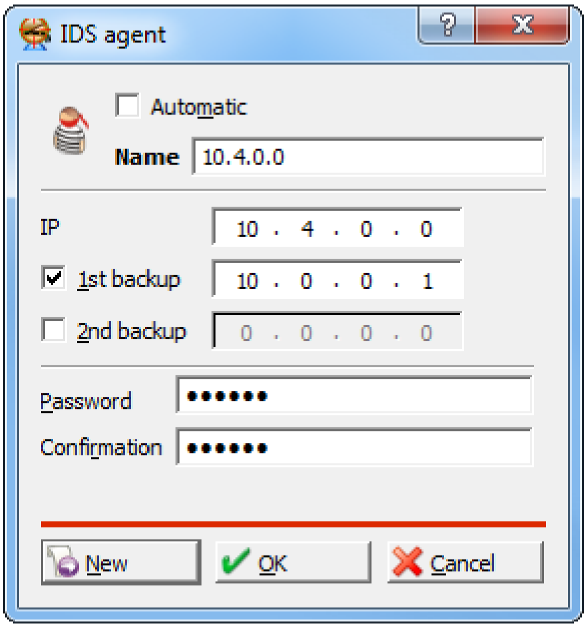
State: State where the company is located

Country: Country where the company is located

The fields: Common Name, Email address, Company, Department, City, State and Country refer to the person who the certificate was issued to.

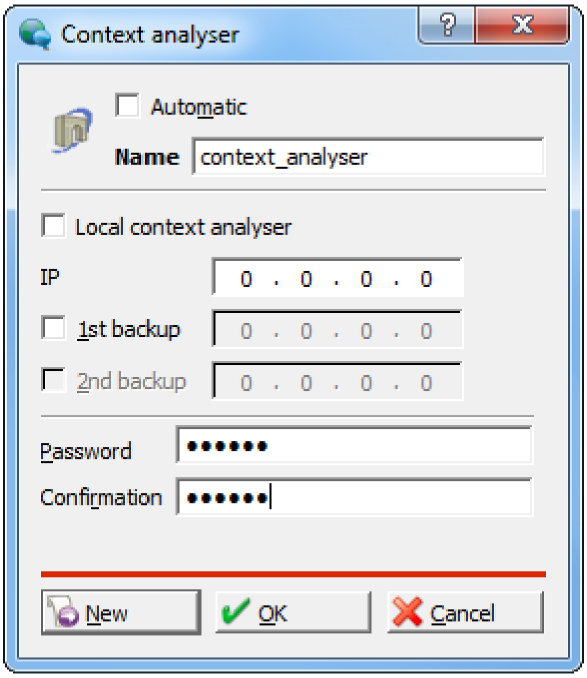
For a user authenticated through the certification authority be considered as Pseudo-group member all of his X.509 certificate field shall filled in same as the Pseudo-group fields. The Blank fields in a Pseudo-group are ignored in the comparison, so any certificate value to this field will be accepted.

- In order to register an External agent type IDS agent, Context analyzer, Anti-virus, Spam Meter or Remote log servers, shall fill in the following additional fields:



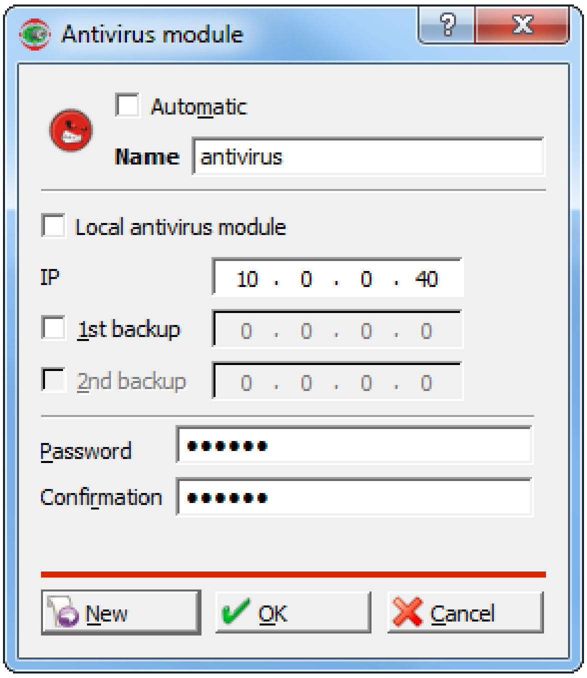
☐ Automatic
Name 10.4.0.0
IP 10 . 4 . 0 . 0
☑ 1st backup 10 . 0 . 0 . 1
☐ 2nd backup 0 . 0 . 0 . 0
Password ••••••
Confirmation ••••••

Image 156 – External agent: *IDS Agent* registration.



☐ Automatic
Name context_analyser
☐ Local context analyser
IP 0 . 0 . 0 . 0
☐ 1st backup 0 . 0 . 0 . 0
☐ 2nd backup 0 . 0 . 0 . 0
Password ••••••
Confirmation ••••••

Image 157 – External agent: *Content Analyzer* registration.



Antivirus module

☐ Automatic

Name antivirus

☐ Local antivirus module

IP 10 . 0 . 0 . 40

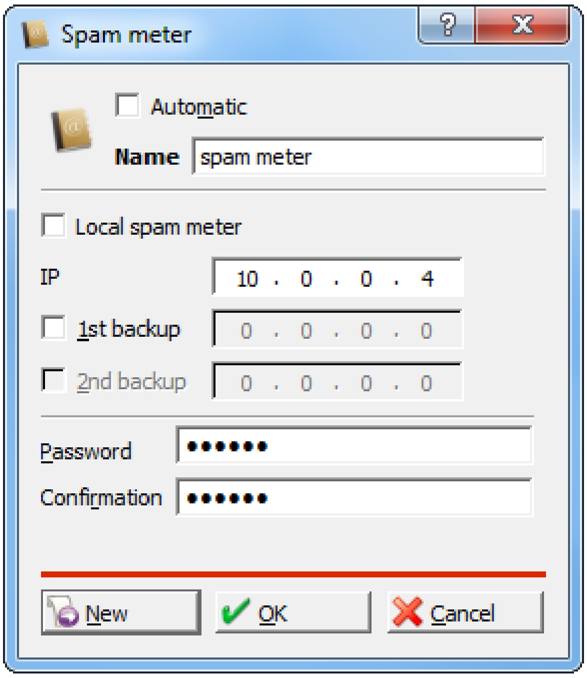
☐ 1st backup 0 . 0 . 0 . 0

☐ 2nd backup 0 . 0 . 0 . 0

Password ••••••

Confirmation ••••••

Image 158 – External agent: *Antivirus module* registration.



Spam meter

☐ Automatic

Name spam meter

☐ Local spam meter

IP 10 . 0 . 0 . 4

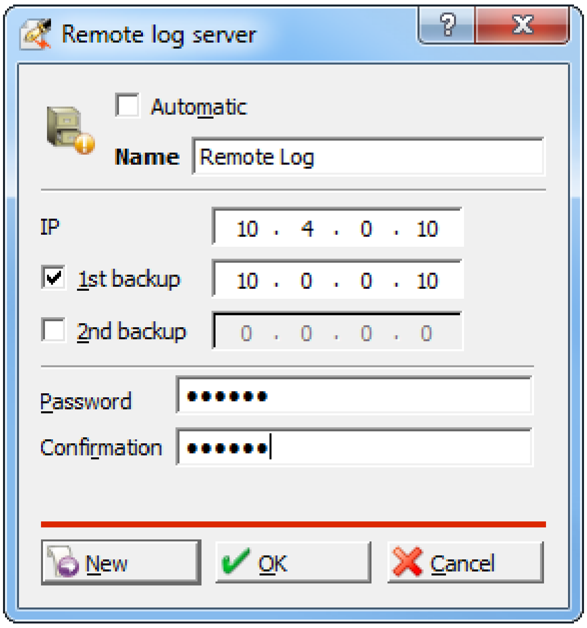
☐ 1st backup 0 . 0 . 0 . 0

☐ 2nd backup 0 . 0 . 0 . 0

Password ••••••

Confirmation ••••••

Image 159 – External agent: *Spam Meter* registration.



Remote log server

☐ Automatic

Name Remote Log

IP 10 . 4 . 0 . 10

☑ 1st backup 10 . 0 . 0 . 10

☐ 2nd backup 0 . 0 . 0 . 0

Password ••••••

Confirmation ••••••

Image 160 – External agent: *Remote log server* registration.

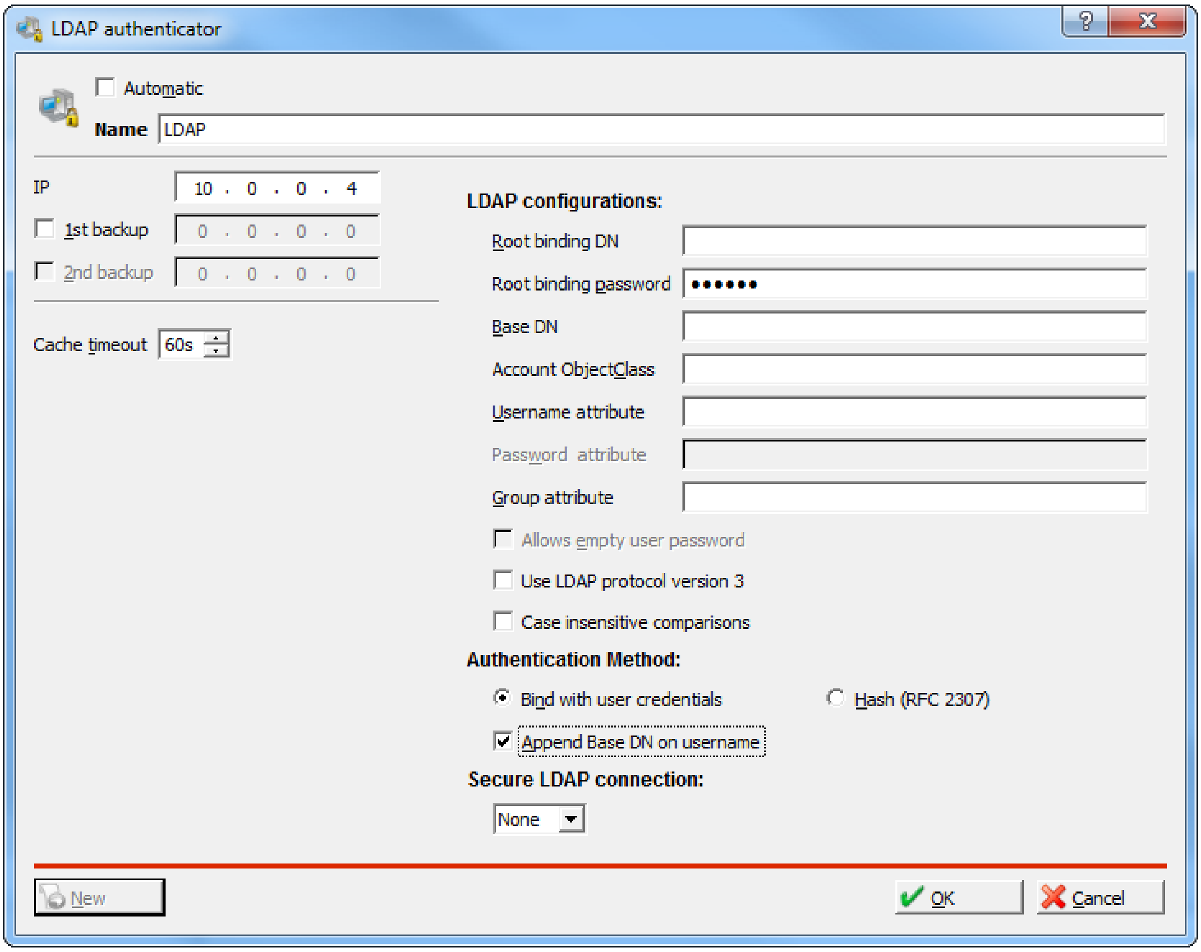
IP: Is the host IP address where the agent is running.

1st Backup and **2nd Backup** : these fields allow specifying up to two address of other hosts that are running the agent and will be used as backup in case the main host goes down.

Password: Is a password used to generate the encryption and authentication Keys used in the communication with the agent. This password shall be same as the one configured in the agent.

Confirmation: This field is used only to verify if the password was entered correctly. It shall be entered exactly as in the password field.

In order to register an external agent Authenticator LDAP type, the following field shall be filled in:


LDAP authenticator
LDAP configurations:
Root binding DN
Base DN
Account ObjectClass
Username attribute
Password attribute
Group attribute
Authentication Method:
Secure LDAP connection:
New
OK
Cancel

☐ Automatic
Name LDAP
IP 10 . 0 . 0 . 4
☐ 1st backup 0 . 0 . 0 . 0
☐ 2nd backup 0 . 0 . 0 . 0
Cache timeout 60s
Root binding password ••••••
☐ Allows empty user password
☐ Use LDAP protocol version 3
☐ Case insensitive comparisons
● Bind with user credentials ○ Hash (RFC 2307)
☑ Append Base DN on username
Secure LDAP connection: None

Image 161 – External agent: LDAP authenticator registration.

IP: The host IP address where the agent is running.

1st Backup and 2nd Backup : These fields allow specifying up to two addresses of other hosts that are running the LDAP server and will be used as backup in case the main host goes down.

Cache timeout: Every time a successful authentication is made, the firewall keeps in memory the received data form the user and the agent. In the following authentications, the firewall has all the necessary data and does not need to consult the agent. This allows a great performance gain.

This parameter allows setting the time in seconds that the firewall has to keep the authentication information in memory. For more information, see the chapter titled: **Working with the proxies.**

LDAP configurations: In this set of field shall specify the LDAP server configurations that will be used to make the authentications. The description of each field can be seen bellow:

Root binding DN: User DN used by the firewall to make queries

Root binding password: User password

Base DN : DN to start a search

Account objectclass: *Objectclass* value that identify objects in valid accounts

Username attribute: Attribute where the user name is found

Password attribute: Attribute where the user password is found

Group attribute: Attribute where the user group is found

Allows empty user password: Allows passwords in blank for the user when is checked

Use LDAP protocol version 3: Enables the use of LDAP protocol version 3

Ignore sensitive case in comparison: Allows that sensitive case in comparisons be treated as the same.

Authentication Method: This field specifies if the firewall shall find a password or connect in LDAP base with the credentials to validate it.

Bind with user credentials: Allows the user to authenticate using user credentials.

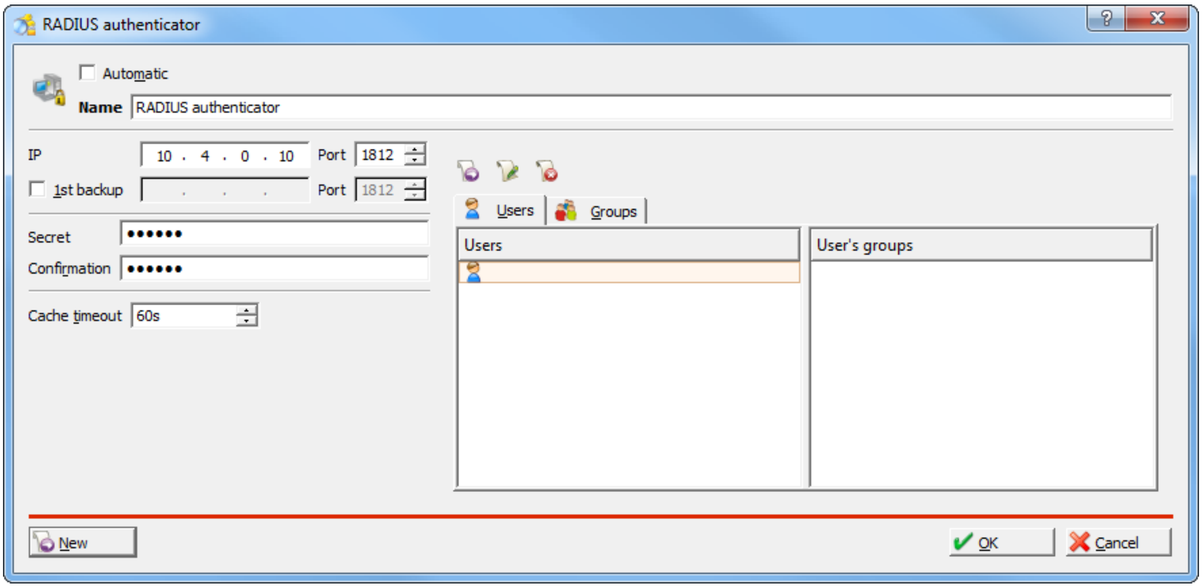
Hash (RFC2307): Allows authentication through Hash mode (RFC2307).

Append Base DN on username: Allows adding DN base to user name in the authentication

Secure LDAP connection: This field specifies if the connection to the LDAP server will be encrypted or not. It has the following options:

- **SSL**: specifies that the firewall will use an encrypted connection via SSL;
- **TLS**: specifies that the firewall will use an encrypted connection via TLS;
- **None**: Specifies that the firewall will not use encryption when connecting to the LDAP server;

In order to register an external agent **Radius Authenticator** type, the following fields shall be filled in:



☐ Automatic

Name: RADIUS authenticator

IP: 10 . 4 . 0 . 10 Port: 1812

☐ 1st backup: . . . Port: 1812

Secret: ••••••

Confirmation: ••••••

Cache timeout: 60s

Image 162 – RADIUS authenticator register.

IP: The host IP address where the agent is running.

Port: The port number where the RADIUS server will be running the authentications requests.

1st Backup: This field allows specifying up to two addresses of other hosts that are running the RADIUS server and will be used as backup in case the main host goes down.

Secret: Is the shared secret used in the RADIUS server.

Confirmation: This is used only to verify if the *secret* was entered correctly. It shall be entered exactly as in the *secret* field.

Cache timeout: Every time is made a successful authentication the firewall keeps in memory the received data form the user and the agent. In the following authentications, the firewall has all the necessary data and does not need to consult the agent. This allows a great performance gain.

This parameter allows setting the time in seconds that the firewall has to keep the authentication information in memory. For more information, see the chapter titled: **Working with the proxies.**

.

Users: This field is used to register and subsequently associate specific RADIUS user with the firewall access profile,

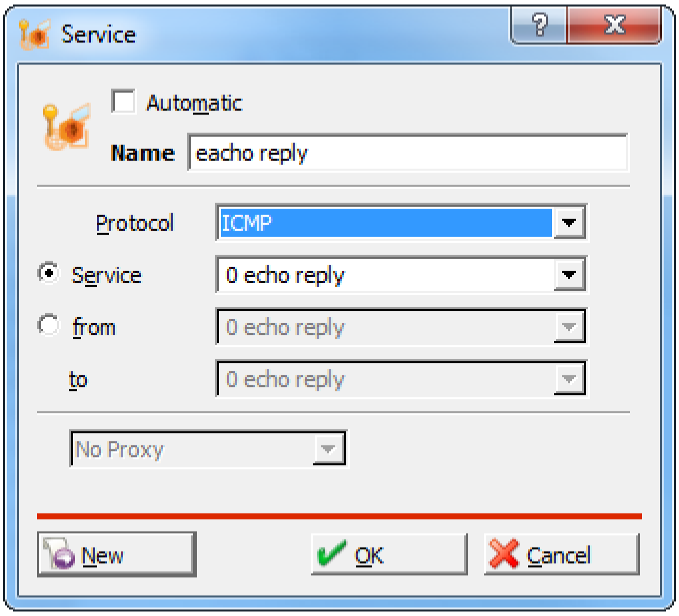
Groups: This field is used to register and associate RADIUS specific groups with the firewall access profile, once with this protocol it is not possible for the firewall to get a completely list of groups.

There is a group named ***RADIUS USERS,*** generated automatically by the firewall that can be used to relate the RADIUS users with a specific access profile. All authenticated users in a specific Radius sever are considered as the belonging to this group. This way, in case the user want to use a single access profile to all users, it is not necessary register any user or group.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, you shall click on ***OK*** to make the inclusion or change of the set.   To cancel the made changes or the inclusion, click on ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number

Adding / Editing service



Service

☐ Automatic

Name: eacho reply

Protocol: ICMP

● Service: 0 echo reply

○ from: 0 echo reply

to: 0 echo reply

No Proxy

Image 163 – Adding and editing the *service*..

In order to register an entity of type *service*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

Protocol: Is the protocol associated to service. (TCP, UDP, ICMP or other)

Service: Is the number that identifies the service. In case the TCP and UDP protocol, this number is the Destination port. In case the ICMP is the service type and in case of other protocols is the protocol number. For each protocol, the firewall has a list of values associated to it, in order to facilitate the service creation. However, is possible to put values that do not belong to the list, simply typing them in this field.

In case the user want to specify the range value, instead of a single value, shall click next to the names ***From*** and ***To*** and specify the smallest range value in ***From*** and the largest in ***To.*** All the understanding values between this two, will be considered as making part of the service.

Proxy: This field can be enabled only for the TCP and UDP protocols, and it also allows to specify if the connection that fits in this service, will be automatically diverted to one of the Aker Firewall transparent proxies or not. The standard value is ***No Proxy***, which means the connection shall not be diverted to any Proxy. When the TCP protocol is selected, the other options are ***SMTP Proxy, Telnet Proxy, User Proxy, HTTP Proxy and POP3 Proxy*** that divert to the SMTP, Telnet, and FTP Proxies. The proxies created by the user are diverted to HTTP and POP3. When the UDP protocol is selected, the other options are ***RPC Proxy,*** which divert to the RPC proxy, and ***User Proxy.***

The Telnet service is associated to port 23, the SMTP to port 25, the FTP to port 21, the HTTP to port 80 and the POP3 to port 110. Is possible to specify connections from any other ports to be diverted to one of this proxies, however, this should not be done unless the user has proper knowledge about the implications.

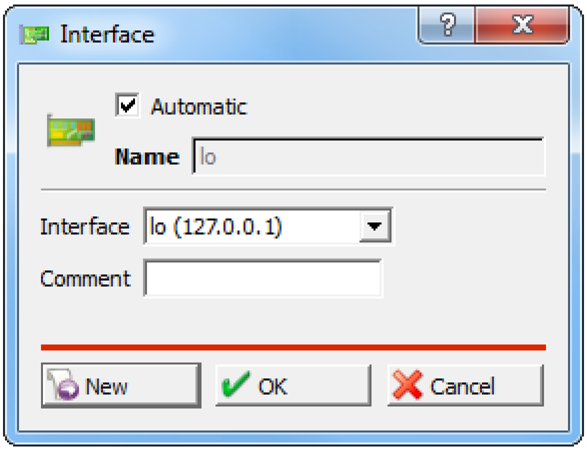
In case the specified connection has been diverted to a proxy, it may be necessary to define the context parameters that will be used by the firewall to this service. In casa is necessary, at the moment that the proxy is selected, the window will be expanded to show the additional parameters that shall be configured.

The parameters explanation of each of the standard proxy contents, is found in the chapters titled: ***Configuring the SMTP proxy, Configuring the Telnet Proxy, Configuring the FTP proxy, Configuring the POP3 proxy, configuring the RPC proxy and DCE-RPC proxy***. The HTTTO proxy does not have configurable parameters and its settings are described in the chapter ***configuring the Web Filter***. For more information about transparent proxies and context, see the chapter titled ***Working with proxies.*** Proxies defined by the user are only useful to the developers.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, shall click on ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, click on ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number

Adding / editing interfaces



☑ Automatic

Name lo

Interface lo (127.0.0.1)

Comment

Image 164 – *Interface* Adding and editing

In order to register an entity of type *Interface*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

Interface: Is the network adapter name that will be associated to the Interface entity. A list with all Firewall network adapters and IP address of each of them will be displayed automatically.

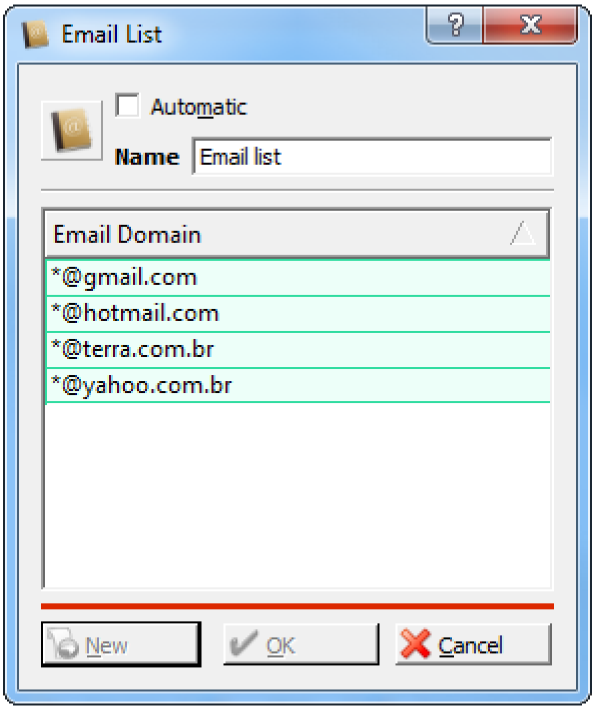
Comment: Is a text field used only for documentation purposes.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, shall click ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, click on ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number

Adding / editing Email list

Email list are entities used in MSN proxy with the purpose of define which people a specific user is allowed to chat through the MSN Messenger.



☐ Automatic

Name: Email list

Email Domain
*@gmail.com
*@hotmail.com
*@terra.com.br
*@yahoo.com.br

Image165 – *Email list* adding and editing.

In order to register an entity of type *Email list*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

The list shall have just “enter or (\n)” with separators on the mailing list.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Email Domain: This field is composed by e-mails or domains that will be part of the list. Is possible to specify a complete email or use the *** *symbol*** to represent any character. The following options are valid emails.

= *@* – Corresponds to any email.

= ***@aker.com.br** – Corresponds to all the emails from *aker.com.br* domain.

To perform any operation on an email or domain, you shall right-click on it and choose one of following the options displayed in the menu:

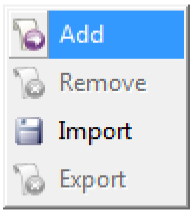


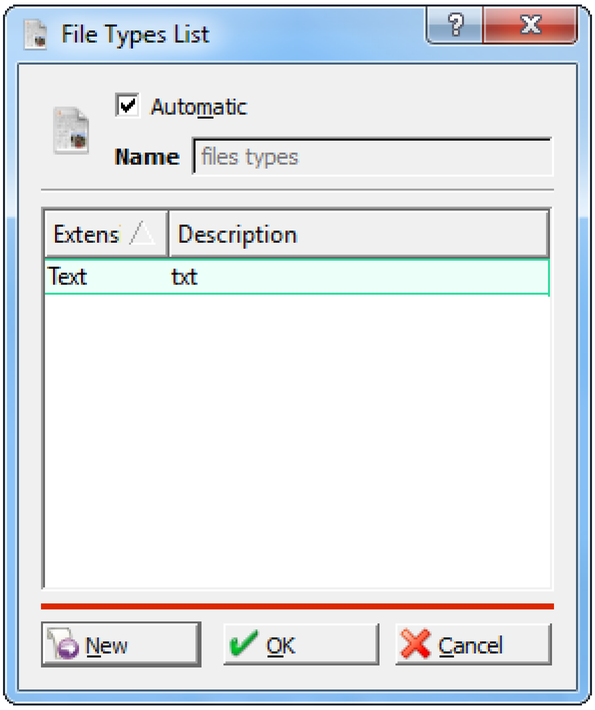
Image 166 – Option to perform an operation about an email or domain.

- **Add:** This option allows to add a new address;
- **Remove**: This option allows to remove an address;
- **Import:** This option imports an email list form the **.ctt file** (formed of Messenger contacts) or **.txt** (text file with an email per line);
- **Export:** This option exports an email list to a **.ctt file** (formed of Messenger contacts) or **.txt** (text file with an email per line);

The list shall have just “enter or (\n)” with separators on the mailing list.

Adding / editing File types list

File types list are entities used in MSN proxy with the purpose of define which files type can be send and received through the MSN Messenger.



☑ Automatic

Name files types

Extens	Description
Text	txt

Image 167 – File types list

In order to register an entity of type *File list*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible specifying this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

To perform any operation on any entry from the list shall right-click on and choose the desired option in the displayed menu. The following options will be available:

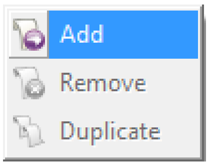


Image 168 – Option to perform an operation (List entry).

Add: Includes a new file type

Remove: Removes a selected file from the list

Duplicate: Creates a new list entry, same as the selected entry

For each entry, the following fields shall be filled in:

- **Extension:** File extension without dot. Ex.: zip, exe, etc.
- **Description:** Brief description of the associated type to the extension.

Adding / editing Counters

Counters are entities used in the filtering rules with the purpose of gather statistics about the network traffic. A counter can be used in several filtering rules. The traffic which fits in each of these rules is summarized by the counter. For more information about its use see the chapter titled: ***States Filter*** and ***Visualizing statistics*.**

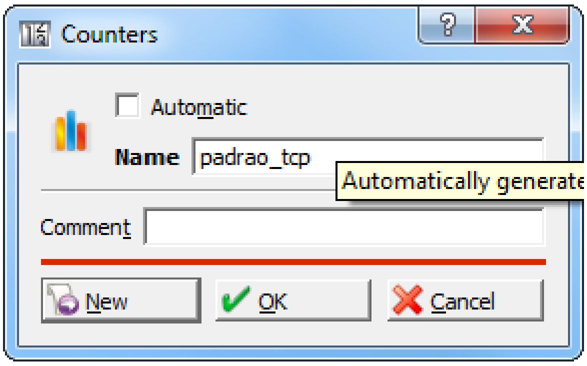


Image 169 – Counters

In order to register an entity of type *Counter*, the following fields shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

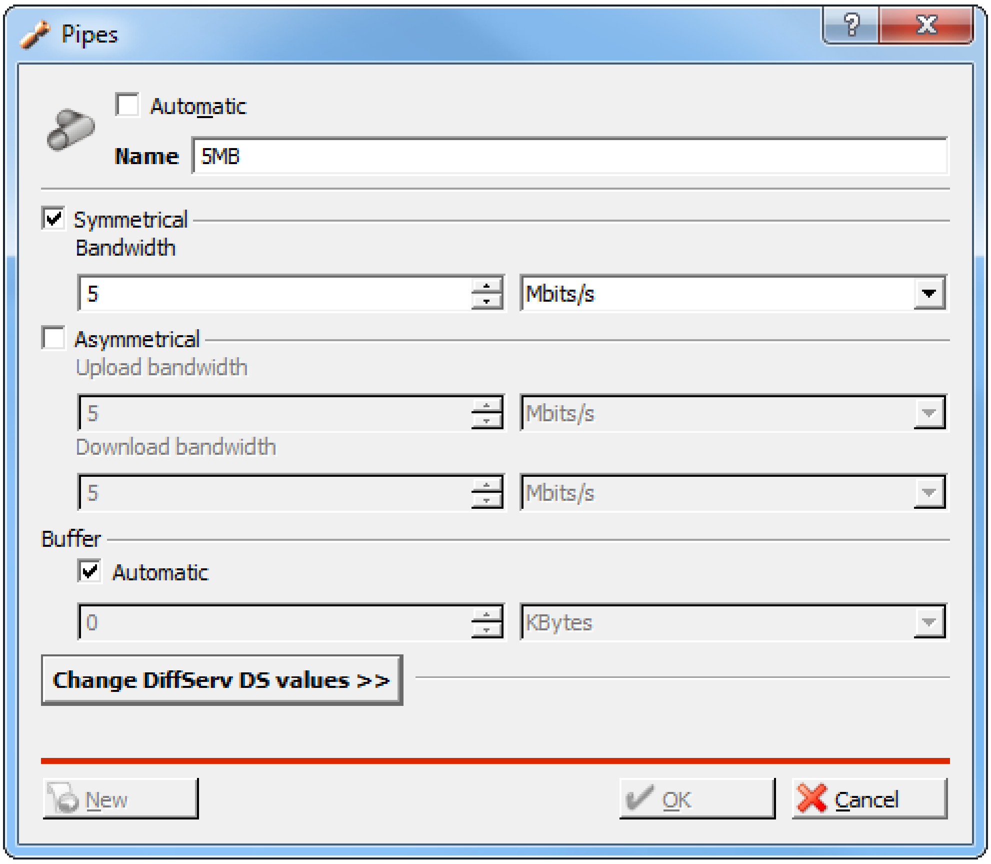
Comment: Is a text field used only for documentation purposes.

After all the fields are filled in and all the networks and hosts that shall make part of the set are selected, you shall click on ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, click on ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number.

Adding / editing Pipes

Pipes are entities used in the filtering rules with the purpose of limit the bandwidth of specific services, hosts, networks and/or users. Its use will be described in the chapter: **States Filter**.



☐ Automatic

Name 5MB

☑ Symmetrical

Bandwidth 5 Mbits/s

☐ Asymmetrical

Upload bandwidth 5 Mbits/s

Download bandwidth 5 Mbits/s

Buffer

☑ Automatic

0 KBytes

Image 170 –*Pipes* entity registration.

In order to register an entity Pipes type, the following field shall be filled in:

Name: Is the name which the host will be referenced by the firewall. It is possible to specify this name manually or let it be assigned automatically.

Uppercase and lowercase letters are considered different in the entities name. This way, is possible the existence of many entities composed of names with the same letters, but with different combinations of uppercase and lowercase letters, The Aker, AKER and aker entities are considered different.

Icon: is the icon that appears associated with the hosts in all references. To change it, just click on the drawing of the current icon. The firewall will show a list with all of the possible icons to represent the hosts. To choose between them just click on the desired icon and click on the ***OK*** button**.** In case you do not want to change it after see the list, just click on ***Cancel***.

Bandwidth: Is a text filed used to designate the bandwidth (maximum transmission speed in bits per second) of this *Pipe*. This band will be shared among all the connections which use this *Pipe.* The convenient unit of measurement shall be chosen.

Upload bandwidth: Maximum transmission speed in bits per second defined to make an upload.

Download bandwidth: Maximum transmission speed in bits per second defined to make a download.

Buffer: Is the text field used to designate the buffer size (temporary space used to store data packets that will be transmitted) Using this *Pipe*. The measurement unit shall be chosen. Is possible to specify the size manually or let it be assigned automatically.

The *automatic* option allows choosing between two operations modes: if it is checked, the assignment will be automatically, or manual.

After all fields are filled in and all networks and hosts that shall be part of the set are selected, shall click on ***OK*** to make the inclusion or change of the set. To cancel the made changes or the inclusion, click on ***Cancel***.

To facilitate the inclusion of many hosts, there is a button called **New** (which will not be enabled during an edition). When clicked, this button will make the host include the data filled in and keep the host inclusion window opened where it will be ready for a new inclusion. This way, is possible to register quickly a large number.

6.3. Using the text interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action)*. The only non-available options are the services creation that uses transparent proxies and the pseudo-group editing of a certification authority.

Program location*: /aker/bin/firewall/fwent*

Syntax:

Usage: fwent help

fwent show

fwent remove *<name>*
fwent add host *<name> <IP*
fwent add network *<name> <IP> <mask>*
fwent add set <name> *[<entity1> [<entity2>] ...]*
fwent add host_ipv6 *<name> <ipv6>*
fwent add network_ipv6 *<name> <ipv6> / <prefix>*
fwent set_ipv6 *<name> [<entity1> [<entity2>] ...]*
fwent add authenticator*<name><IP1>[<IP2>][<IP3>]<password> <t. cache>*
fwent add token *<name><IP1>[<IP2>][<IP3>]<password><t. cache>*
fwent add ldap *<name><IP1>[<IP2>][<IP3>]<root_dn><root_pwd>*

<base_dn><act_class><usr_attr><grp_attr>
<<pwd_attr>|*<-bind> >< <-ssl>*|*<-tls>*|*<-none>>*
< <-no_pwd>|*<-pwd> > <t.cache>*
< <-append_dn> | *<-no_append_dn> >*
< <-ldap_v3> | *<-no_ldap_v3> >*
< <-case_sensitive> | *<-case_insensitive> >*

fwent add radius *<name> <IP1> <port1> [<IP2> <port2>] <password> <t.cache>*
fwent add antivirus *<name> <IP1> [<IP2>] [<IP3>] <password>*
fwent add ids *<name> <IP1> [<IP2>] [<IP3>] <password>*
fwent add spam-meter *<name> < <local>* | *<IP1> [<IP2> [<IP3> <password> >*
fwent add analyser-url *<name> <IP1> [<IP2>] [<IP3>] <password>*
fwent add interface *<name> <device> [<comment>]*
fwent add counter *<name> [<comment>]*
fwent add service *<name> [TCP* | *UDP* | *ICMP* | *OTHER] <value>[..<value>*
fwent add ca *<name> <file with certificate root> <URL with CRLs>:*
fwent add pipe *<name> <band in Kbits/s> [<queue length > <bytes*|*pacts>]*

fwent add remote_log *<name> <IP> [IP] [IP] <password>*
fwent add quota *<name> [kbytes <max kbytes>] [seconds <max seconds>] <type>*
fwent *– Text interface to entities configuration*

Program help:

add *= adds a new entity*
remove *= removes an existing entity*
help *= shows this message*

remove / add:
name *= entity name to be created or deleted*

To add:

IP *= host or network IP address*
mask *= entity network mask = entity name to be added to the set*

(OBS: Only the entities host and network type are allowed to be part of the set)

password *= it is the access password*
t. cache *= time in seconds of an entry in the authenticator cache*

TCP *= service uses TCP protocol*
UDP *= service uses UDP protocol*
ICMP *= service uses ICMP protocol*
OTHER *= service uses a different protocol from the ones above*

value *= Number that identifies the service. For TCP and UDP protocol is the port value associated to service. For ICMP is the service type and in case of other protocol is its own number. A range can be specified through the notation value1..value2, which means the range value is understood between value 1 and 2.*

To add ldap:

root_dn *= User DN used by the firewall to queries*
root_pwd *= this user password*
base_dn *= DN to start the search*
act_class*= objectclass value that identify objects of valid accounts*
usr_attr *= the attribute where the user name is found*
grp_addr *= the attribute where the user group is found*
pwd_addr *= the attribute where user password is found*
-bind *= does not try to seek the password, instead connects in the base*
*-**append_dn*** *= adds DN base to user name*
-ldap_v3 *= assigns which enables or not the LDAP protocol version 3*
*-**no_ldap_v3*** *= does not use LDAP protocol version 3*

case_sensitive *= allows the distinction between lowercase and uppercase characters*

case_insensitive *= ignores lowercase and uppercase in comparison*

LDAP with user credentials to validate it.
-ssl *= uses encrypted connection via ssl*
-tls *= uses encrypted connection via tls*
*-**none** = does not use encrypted connection*
-no_pwd *= allows blank passwords to user*
-pwd *= does not allow blank password*

1st Example :(Visualizing the entities defined in the system)

```
#fwent show


Hosts:
---------
cache 10.4.1.12
firewall 10.4.1.11
Network:
------
AKER 10.4.1.0 255.255.255.0
Internet 0.0.0.0 0.0.0.0
Set:
----------
Internal hosts cache firewall
Authenticators:
---------------
Authenticator NT 10.0.0.1 10.0.0.2 600
Unix 192.168.0.1 192.168.0.2 192.168.0.3 600
Authenticator token type:
-----------------------------
Authenticator token 10.0.0.1 10.0.0.2 600
IDS Agents:
------------
IDS Agent 10.10.0.1
Antivirus:
-----------
local  Antivirus 127.0.0.1
Services:
---------
echo reply ICMP 8
echo request ICMP 0
ftp TCP 21
snmp UDP 161
telnet TCP 23
Interfaces:
----------
External Interface xl0
Internal Interface de0
```

2nd Example: (registering an entity *HOST*)

```
#/aker/bin/firewall/fwent add host_sever_1 10.4.1.4

Entity included
```

3rd Example: (registering an entity *NETWORK*)

```
#/aker/bin/firewall/fwent add network Network_1 10.4.0.0 255.255.0.0
Entity included
```

4th Example: (registering an entity *SERVICE*)

```
#/aker/bin/firewall/fwent add service DNS UDP 53
Entity included
```

5th Example: (registering an entity *AUTHENTICATOR*)

```
#/aker/bin/firewall/fwent adds authenticator "Authenticator Unix" 10.4.2.2
password_123 900
Entity included
```

The use of **""** around the entity name is mandatory when add or remove entities whose name contains spaces.

6th Example: (adding an entity *SET*, which members are cache hosts and firewall, previously defined)

```
#/aker/bin/firewall/fwent add set "Test set" firewall cache
Entity included
```

7th Example: Adding an entity interface, without specifying a comment)

```
#/aker/bin/firewall/fwent add interface "Interface DMZ" fxp0
Entity included
```

8th Example: (adding an entity authenticator token, using a primary and secondary host, as backup)

```
#/aker/bin/firewall/fwent add token "Authenticator token" 10.0.0.1 10.0.0.2 password
600
Entity included
```

9th Example: (removing an entity)

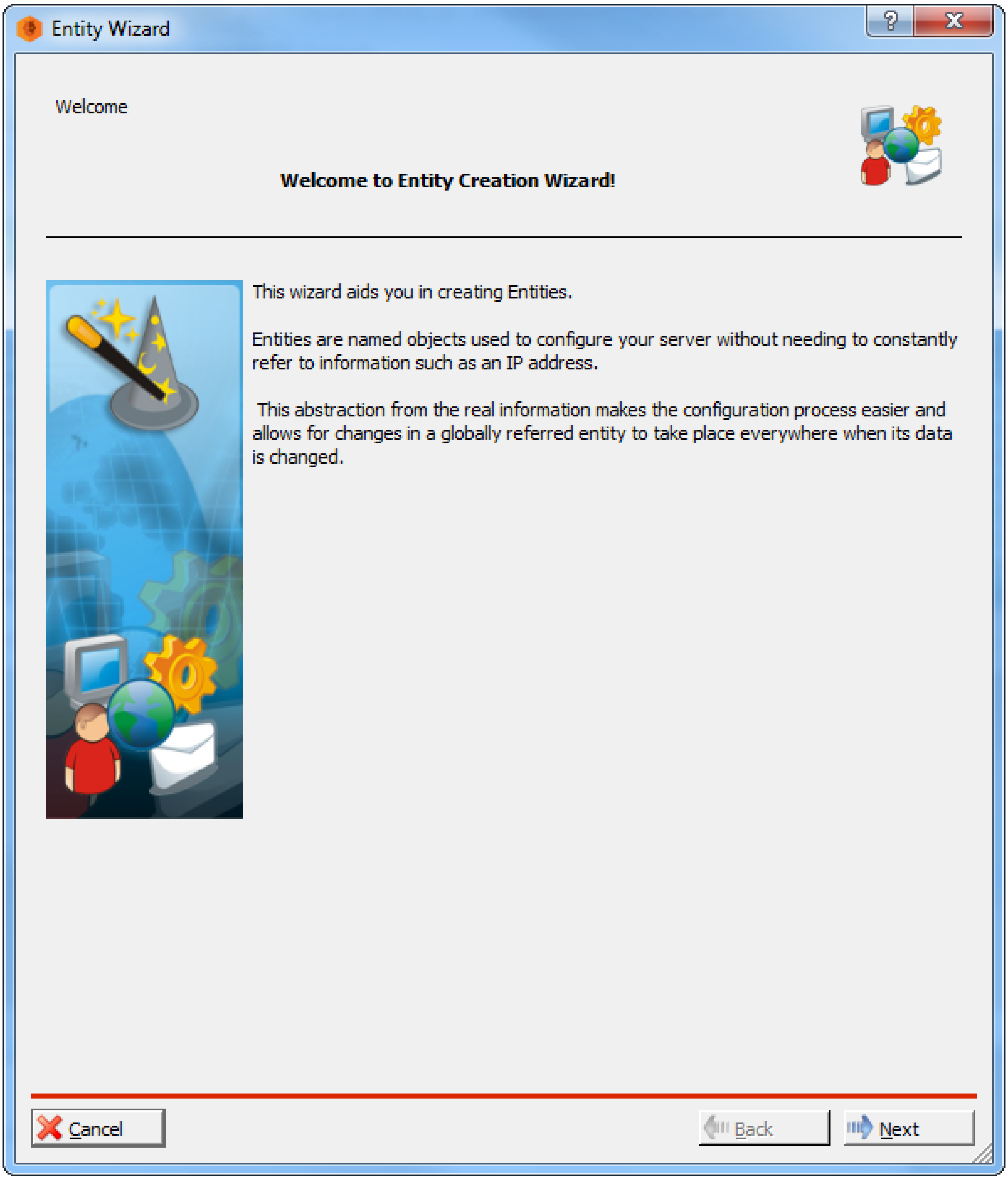
```
#/aker/bin/firewall/fwent remove "Authenticator Unix"
Entity included
```

6.4. Using the entity wizard

You can activate the entity wizard by clicking on the icon, located at the external part on the left side of the entity window. Its goal is to simplify the task of entities creation, and it can be used whenever is required. It consists of several windows displayed in classes, depending on the type of entity to be created.

Its use is extremely simple as it is explained bellow:

1st – The first window will show a brief explanation of the procedures to be made:



Welcome

Welcome to Entity Creation Wizard!

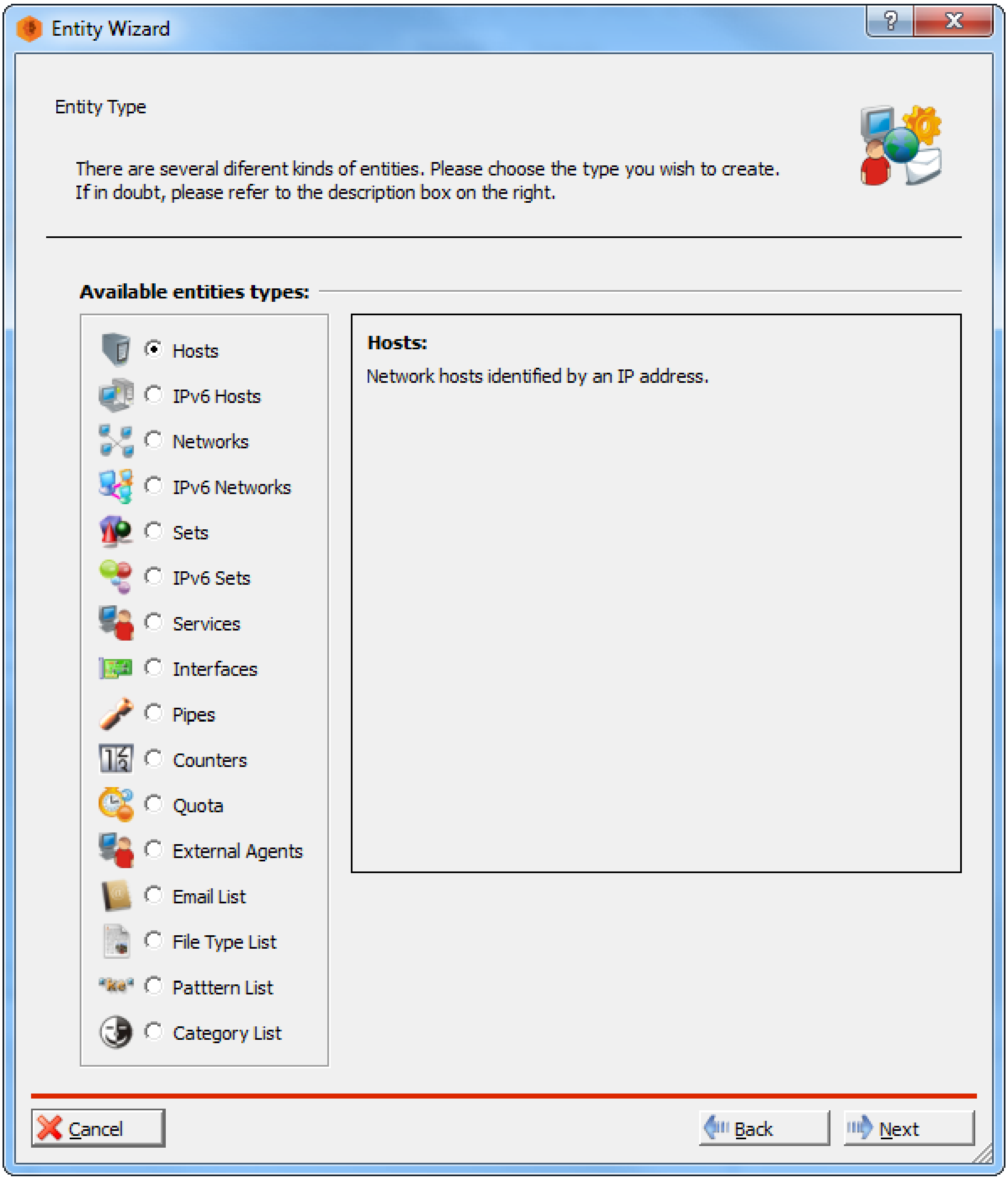
This wizard aids you in creating Entities.

Entities are named objects used to configure your server without needing to constantly refer to information such as an IP address.

This abstraction from the real information makes the configuration process easier and allows for changes in a globally referred entity to take place everywhere when its data is changed.

Image 171 – Welcome message in the *Entity wizard.*

2nd – Choose entity type. In the second window, the type of entity to be registered shall be chosen:



Entity Type

There are several diferent kinds of entities. Please choose the type you wish to create.
If in doubt, please refer to the description box on the right.

Available entities types:

- ● Hosts
- ○ IPv6 Hosts
- ○ Networks
- ○ IPv6 Networks
- ○ Sets
- ○ IPv6 Sets
- ○ Services
- ○ Interfaces
- ○ Pipes
- ○ Counters
- ○ Quota
- ○ External Agents
- ○ Email List
- ○ File Type List
- ○ Patttern List
- ○ Category List

Hosts:

Network hosts identified by an IP address.

Image 172 – Choose the entity type.

3rd – Locating the IP address. To register a host shall specify its IP address. In case the user wishes to get this address, the host name shall be informed and right after click on the ***Resolve*** icon:

Resolve

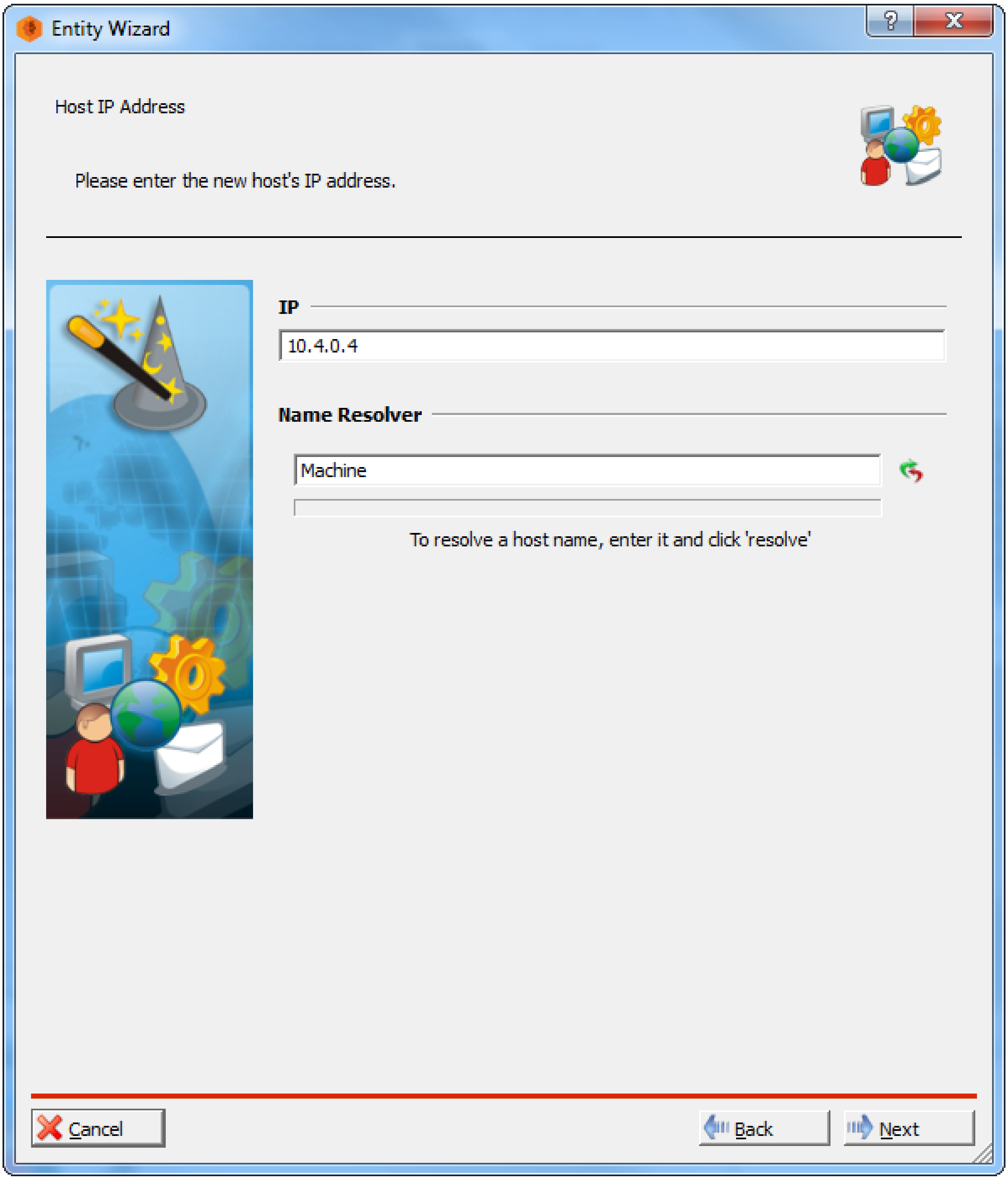
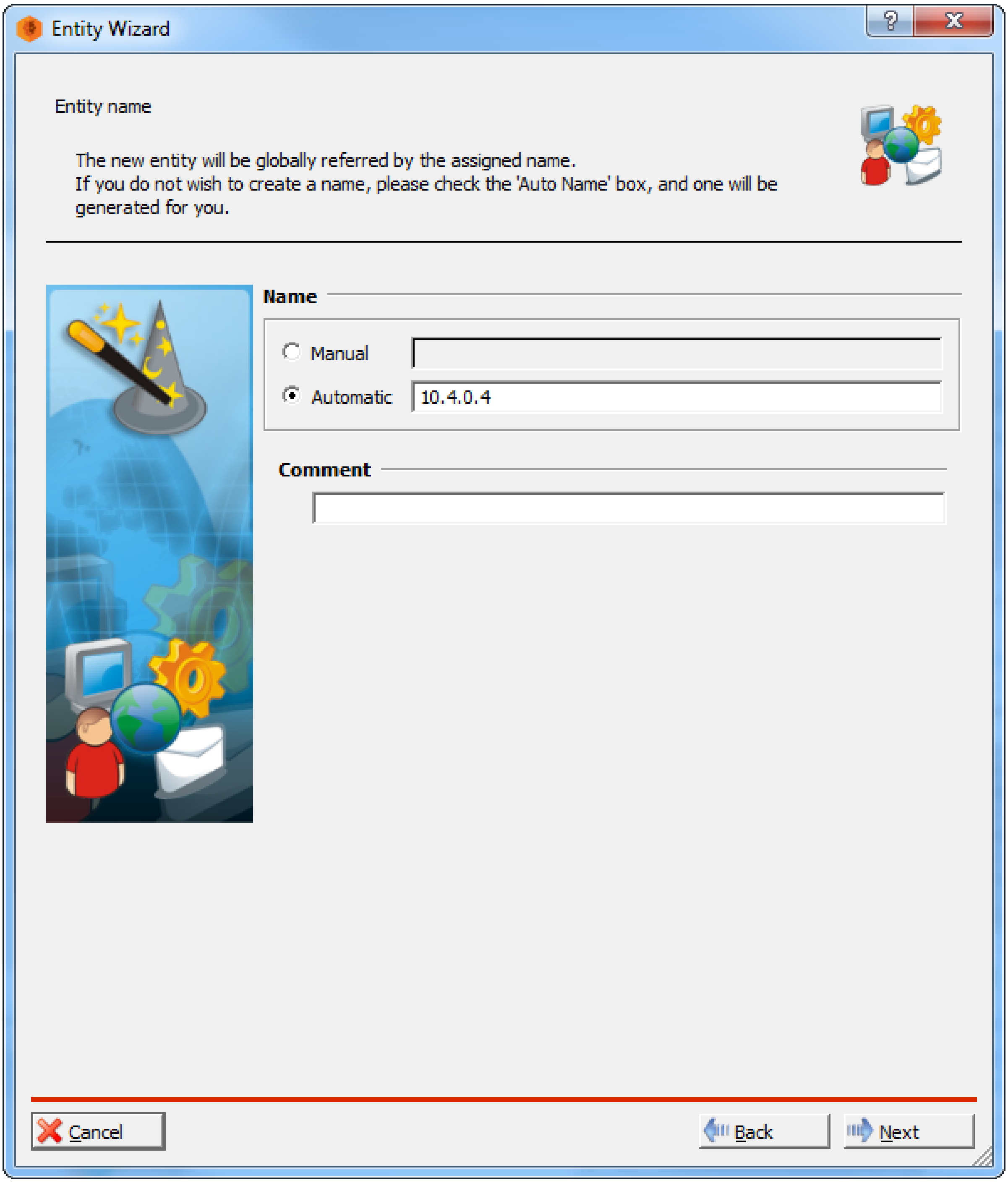

Entity Wizard
Host IP Address
Please enter the new host's IP address.
IP
10.4.0.4
Name Resolver
Machine
To resolve a host name, enter it and click 'resolve'
Cancel
Back
Next

Image 173 – Adding the host IP address.

4th – Entity name assignment. You can choose the name or use the automatic option:



Entity name

The new entity will be globally referred by the assigned name.
If you do not wish to create a name, please check the 'Auto Name' box, and one will be generated for you.

Name

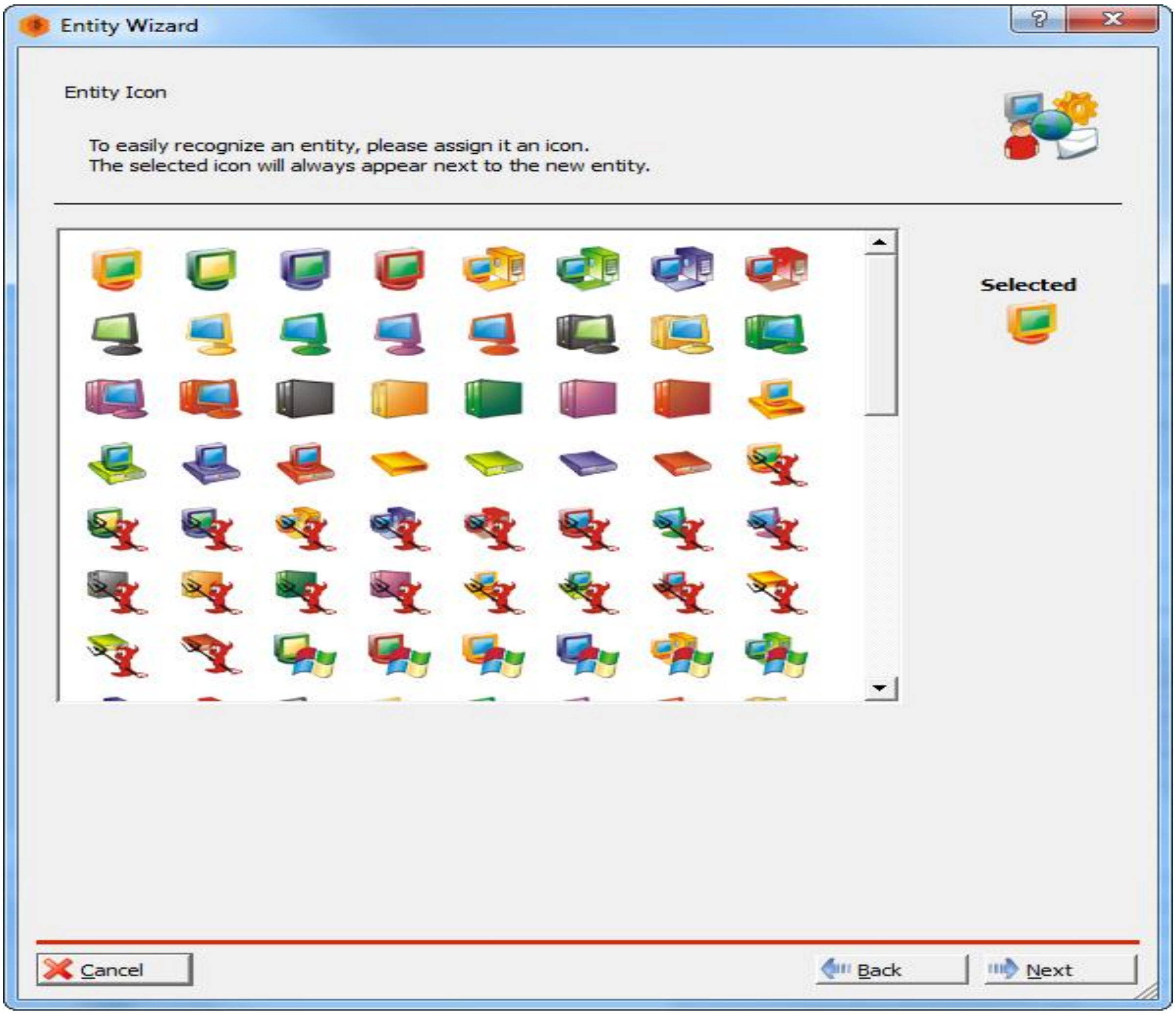
○ Manual

● Automatic: 10.4.0.4

Comment

Image 174 – Entity name assignment.

5th –Choose the entity icon. To choose the entity icon, you shall click on one of the icon in the window. The selected icon will be displayed on the right:

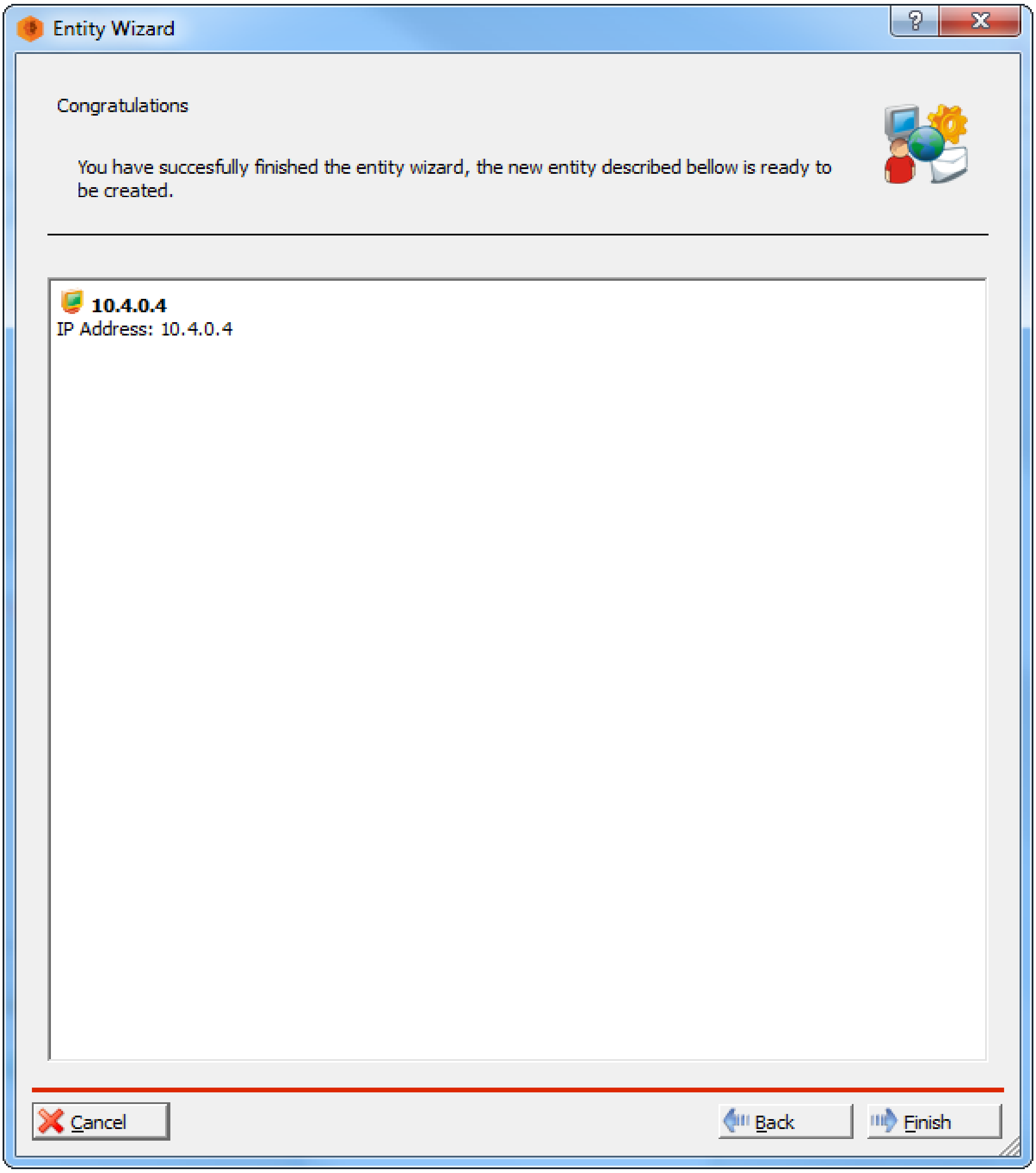


Entity Icon

To easily recognize an entity, please assign it an icon.
The selected icon will always appear next to the new entity.

Image 175 – Choosing the entity icon.

6th – Finishing the registering. A summary of the entity data will be displayed. To finalize the registration simply click on ***Finish****:*



Entity Wizard

Congratulations

You have succesfully finished the entity wizard, the new entity described bellow is ready to be created.

10.4.0.4
IP Address: 10.4.0.4

Image 176 – Finishing entity registration.

Stateful Inspection

7. Stateful Inspection

This chapter will show how to configure the rules that will provide the acceptance or not of connections through the firewall. This module is the most important of the system and is where normally you spend most of the time configuring.

7.1. Planning the installation

What is a packet filter?

A packet filter is the module that will decide if a specific packet can pass through the firewall or not. Let the packet pass means accept a specific service. Blocking a packet means prevent a service to be started.

In order to decide what action to be taken for each packet when it gets to the firewall, the *packet filter* has a set of rules configured by the system administrator. For each packet that gets to the firewall, the *packet filter* runs through this set of rules, in the same order as it was created, verifying if it matches to any of the rules. If it match to one rule then the defined action for this specific packet will be performed.

What is Aker Firewall stateful inspection?

A traditional packet filter relies all of its actions exclusively in the set of rules configured by the administrator. For each packet that will be able to pass through the filter, the administrator has to configure the rules that allow its acceptance. In some cases this is simple, but in others this is not possible to be done or at least unable to perform with the security and flexibility.

Aker Firewall packet filter which is called *Stateful Inspection*, stores status information of all the connections running through the firewall and uses the information together with the rules defined by the administrator at the time to take decision of allow or not the passage of a specific packet. Besides that, unlike a packet filter that bases its decision only on the data contained in the packet header, the *stateful inspection examines data from all* layers and uses all of these data to make one decision.

Let us analyze how this allows the solution of many problems presented by the traditional packet filter.

The problem with the UDP protocol:

To use a UDP service, the client host chooses a port number (which change every time the service is used) and sends a packet to the server host port corresponding to the service. When the server host receives the request, it answers with one or more packets to the client host port. In order to the communication be effective, the firewall shall allow the *request packets of service and response* passage. The problem is the UDP protocol which is not oriented to the connection this means if a specific packet is sent out of context, it is not possible to know if it is a request or a response of a service.

In the traditional packet filters as the administrator cannot know initially, what port will be chosen by the client host to access a specific service, it *can block all UDP traffic or allow the packet passage to all possible ports*. Both options have few problems.

Aker Firewall has the ability to dynamically adapt to traffic in order to solve possible problems. An example is when a UDP packet is accepted by one of the rules configured by the administrator, with this, an entry is added in an internal table, called *stateful table*, so it allows the response packet to the corresponding service can return to the client host. This entry is only active during a short period of time (this time interval is configured through the configuration window, displayed in the chapter titled ***Configuring System Parameters***). This way, the administrator does not need to worry with the UDP response packet, being necessary only to setup the rules to allow the access to the services. It can be easily done, because all services have fixed ports.

The problem with the FTP protocol:

FTP is one the most popular Internet protocols, but is one of the most complexes to be handled by a firewall. Let us analyze its operation:

To access the FTP service, the client host opens a TCP connection to the server host in port 21(the port used by the client is arbitrary). This connection is called control connection. So for each transferred file or for each directory listing, a new connection is established, called data connection. This data connection can be established in two different ways:

1. The server can initiate the connection from the port 20 towards a variable port, informed by the client, through the control connection (this is called **FTP active mode**)
2. The client can open the connection from an arbitrary port to another arbitrary server port (this is called **FTP passive mode**).

In both cases the administrator has no way of knowing which ports will be chosen to establish the data connections and thus, if the administrator wants to use the FTP protocol through a traditional packet filter, he shall release the access to possible ports used by the clients and server hosts. This has serious security implications.

Aker Firewall has the ability to scour the FTP control connection traffic and this way find out what is the type of transfer that will be used (active mode or passive mode) and which ports will be used to establish the data connection. This way, every time the packet filter determinates that a file transfer is performed, it adds an entry in the stateful table allowing the data connection be established. This entry stay active only when the transfer is being performed in case the control connection is opened, providing maximum flexibility and security. In this case to configure the FTP access the user shall add a rule releasing the access to the control connection port (port 21). Everything else is done automatically.

The problem with the Real Audio protocol:

The Real Audio protocol is the most popular sound and video transfer protocol in real time through the internet.

To make an audio and video transmission possible is necessary that the client establishes a TCP connection to the Real Audio server. Beside this connection, to get a better sound quality, the server can open a UDP connection for the client, to a random port informed in real time by client and the client can also open another UDP connection for the server, and also in one random port informed by the server during the connection.

The traditional packets filter does not allow the establishment of the UDP connection from server to client and vice versa, once the ports are not known previously, causing the audio and video quality be reduced.

Aker Firewall stateful filter follows all the negotiation of the Real Audio server with the client, in order to determinate if the UDP connections will be opened and in what ports it will be used to add this information in an entry in its stateful table. This entry in the stateful table is active during the TCP control connection is opened, providing maximum security.

The problem with the Real Video protocol (RTSP):

The Real Video protocol is supported by the firewall. As the Real Audio transfers are controlled by the firewall, allowing the Real Video applications be used with total security.

Mounting filtering rules in a simple packet filter.

Before showing how the Aker Firewall stateful filter configuration works is interesting to explain the basic operation of a simple packet filter:

There are several possible criterions to perform a packet filtering. The address filtering can be considered the simplest of all, because it consists in making a comparison between the packets addresses and the rules addresses. In case the addresses are the same, the packet is approved. This comparison is done as follows:

We shall work with the following rule: All the hosts from the network 10.1.x.x can communicate with the hosts of network 10.2.x.x. We write this rule using the masking concept (for more information, see the chapter titled **Registering entities**). Then we have:

10.1.0.0 & 255.255.0.0 -> 10.2.0.0 & 255.255.0.0

------- Source ------ ------- Destination -------

Now let us apply the rule to a packet which travels from host 10.1.1.2 to host 10.3.7.7. Apply the rule mask to both addresses, the rule and the packet verify if the source and Destination addresses are the same.

For the source address we have:

10.1.0.0 AND 255.255.0.0 = 10.1.0.0 (for rule)

10.1.1.2 AND 255.255.0.0 = 10.1.0.0 (for packet)

Therefore, the two source addresses are alike after applying the mask. Now we shall see to the Destination address:

10.2.0.0 AND 255.255.0.0 = 10.2.0.0 (for rule)

10.3.7.7 AND 255.255.0.0 = 10.3.0.0 (for packet)

As the packet Destination address is not alike to the rule Destination address after applying the mask, by definition, this rule will not apply to this packet.

This operation is made in every address list and Destination and source mask until the end of the list, or until one of the rules apply to the examined packet. A list of rule would have the same form:

10.1.1.2 & 255.255.255.255 -> 10.2.0.0 & 255.255.0.0

10.3.3.2 & 255.255.255.255 -> 10.1.2.1 & 255.255.255.255

10.1.1.0 & 255.0.0.0 -> 10.2.3.0 & 255.255.255.0

10.1.0.0 & 255.255.0.0 -> 10.2.0.0 & 255.255.0.0

Beside the Destination and source address, each IP packet has a protocol and an associated service. This combination of service plus protocol can be used with one more filtering criterion.

The services in the TCP protocol, for instance, they are always associated to a port (for more information, see the chapter titled **Registering entities**). Therefore, it can associate a port list to the addresses as well.

Let us pick up as an example two well-known services, the POP3 and the HTTP. The POP3 is associated to port 110 from sever, and the HTTP is associated to port 80. Therefore, we shall add these ports in the rule format:

```
10.1.0.0   &   255.255.0.0   ->   10.2.0.0   &   255.255.0.0       TCP       80    110

  ------- Source ------                  ------- Destination -------    - Protocol –     --Ports-
```

This rule allows the entire network packet 10.1.x.x to network 10.2.x.x which uses the HTTP or POP3 services to pass through the firewall.

Thus, in a first step compares the rule addresses with the packet. In case this address are equal after the mask applying, compare the protocol and the Destination port in the packet with the protocol and the list of associated ports to the rule.

Thus a set of rules would have the following format:

10.1.1.2 & 255.255.255.255 -> 10.2.0.0 & 255.255.0.0 UDP 53

10.3.3.2 & 255.255.255.255 -> 10.1.2.1 & 255.255.255.255 TCP 80

10.1.1.0 & 255.0.0.0 -> 10.2.3.0 & 255.255.255.0 TCP 21 20 113

10.1.0.0 & 255.255.0.0 -> 10.2.0.0 & 255.255.0.0 ICMP 0 8

Mounting filtering rules for Aker Firewall.

Configure the filtering rules in Aker Firewall is really easy. All area of IP address, masks, protocols, ports are interfaces and are configured in the entities (for more info, see the chapter titled ***Registering Entities***). When a rule is configured is not necessary to worry on which port a specific service uses or which is the IP address of a network. All of it, is already installed. In order to facilitate even more, all the most used Internet services come pre-configured from the factory, so there is no need of spend time searching data of each one of them.

Basically, to register a rule, the administrator has to specify the source and Destination entities, and the service which will be part of the rule. They may specify a source interface for the packets and define in what time the rule will be active, in a weekly timetable. Using this timetable is possible to release certain services in specific times in the day (for instance, release IRC, Chat, and etc.). If a packet gets in a time which the rule is not checked as active, it will be ignored, so the search will continue in the next rule of the list.

The filter operation is simple: the firewall will search one by one the rules defined by the administrator, in the specified order, until the packet fits in one of these rules. From this moment, it will perform the action associated to the rule, which can be accepted, rejected or disposed (these values will be explained in the next topic). In case the search reaches the end of the list and the packet does not fit in any rules, it will be disposed (it is possible to configure actions to be performed in this case, it will be displayed in the chapter titled ***Configuring system actions).***

7.2. Editing a list of rules using the Remote Interface

To gain access to the rules configuration window just need to:

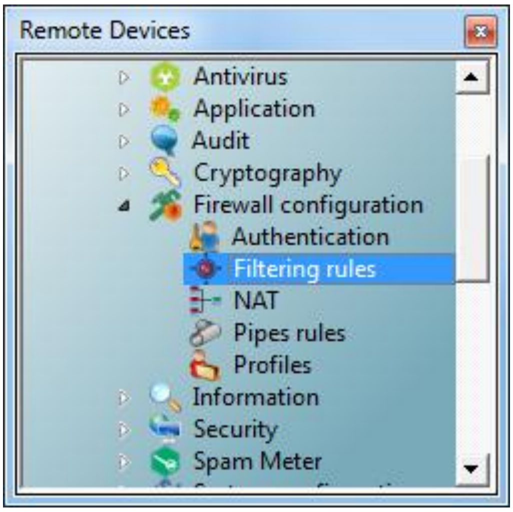
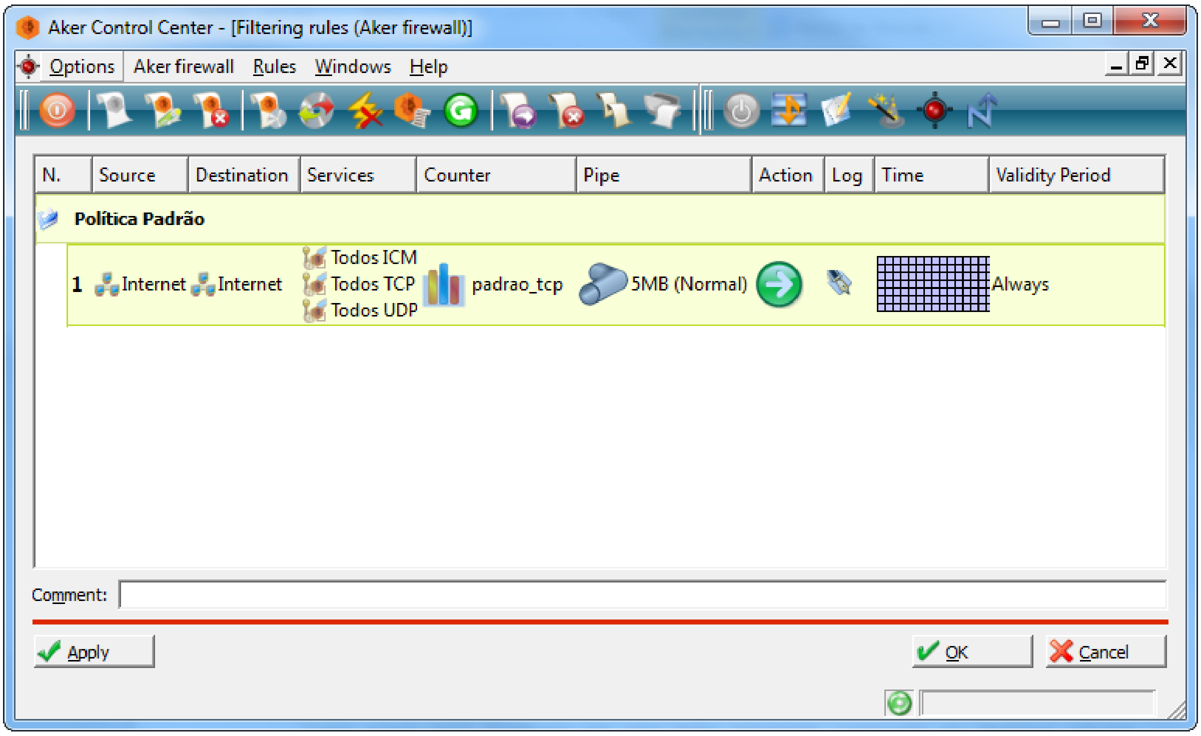

Remote Devices
Antivirus
Application
Audit
Cryptography
Firewall configuration
Authentication
Filtering rules
NAT
Pipes rules
Profiles
Information
Security
Spam Meter

Image 177 – Remote Devices (Access to rules configuration window)

- Click on the *Firewall configuration menu*
- Select Filtering rules.

The filtering rules window


Aker Control Center - [Filtering rules (Aker firewall)]
Options
Aker firewall
Rules
Windows
Help
Comment:
Apply
OK
Cancel

N.	Source	Destination	Services	Counter	Pipe	Action	Log	Time	Validity Period
Política Padrão									
1	Internet	Internet	Todos ICM Todos TCP Todos UDP	padrao_tcp	5MB (Normal)				Always

Image 178 – Filtering rules window.

This Window contains all filtering rules of Aker Firewall. Each rule is displayed in a specific line, consisting of several cells. In case a rule is selected, it will be displayed in a different color.

- The ***OK*** button shall make the rule set to be updated and run immediately.
- The ***Cancel*** button shall make all the made changes be ignored and the window closed.
- The ***Apply*** button shall send all the made changes to the firewall and the window will remain opened.
- Clicking on a rule which has any comment, this comment shall appear at the bottom of the window.

In order to perform any operation in a specific rule, user shall right-click on the field you wish to change. A menu with entities options will appear as in the Image bellow:

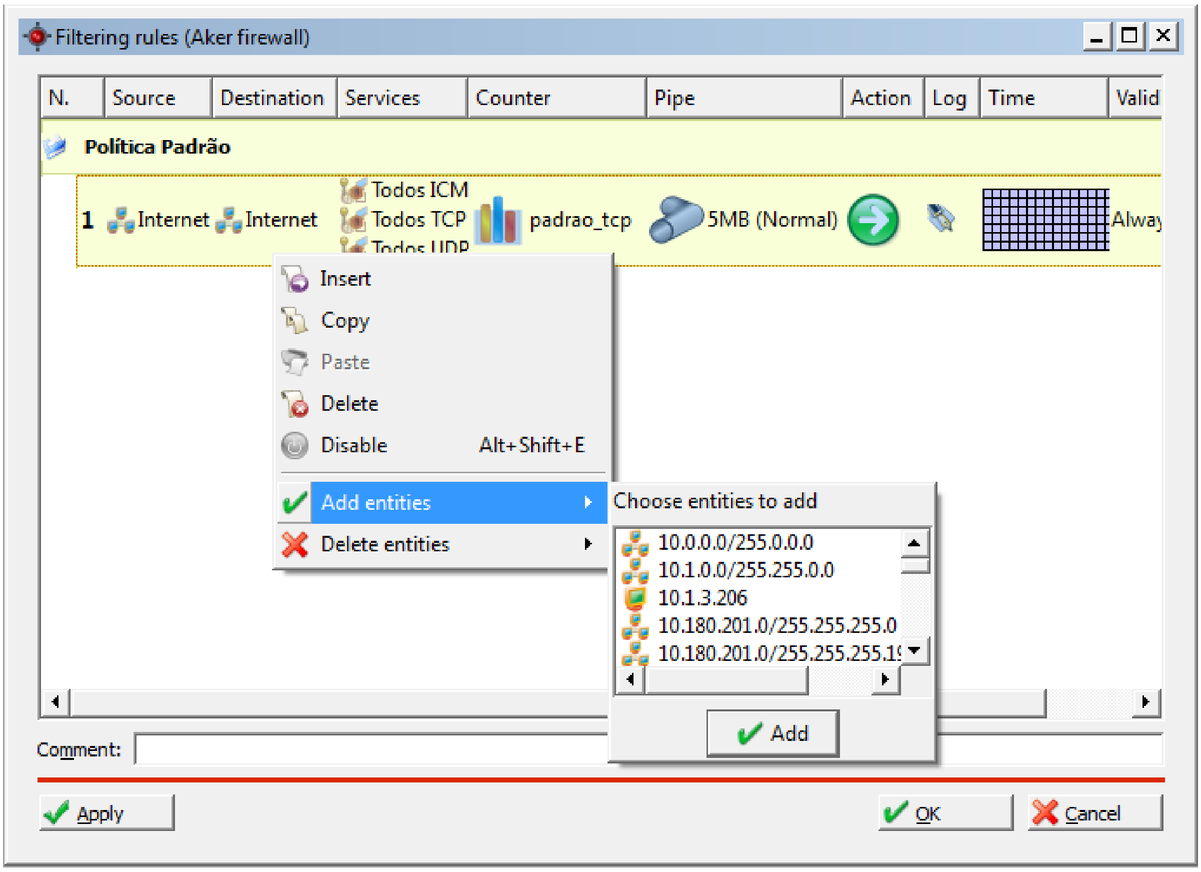

Filtering rules (Aker firewall)
N.
Source
Destination
Services
Counter
Pipe
Action
Log
Time
Valid
Política Padrão
1
Internet
Internet
Todos ICM
Todos TCP
Todos UDP
padrao_tcp
5MB (Normal)
Alway
Insert
Copy
Paste
Delete
Disable Alt+Shift+E
Add entities
Delete entities
Choose entities to add
10.0.0.0/255.0.0.0
10.1.0.0/255.255.0.0
10.1.3.206
10.180.201.0/255.255.255.0
10.180.201.0/255.255.255.1!
Add
Comment:
Apply
OK
Cancel

Image 179 – Menu with entities options regarding to the chosen field.

- **Insert:** Adds a new rule in the list.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes the copied rule.
- **Delete**: Removes the selected rule.
- **Enable/Disable:** Enables or disables a selected rule.
- **Add entities:** Adds a new firewall registered entity in the rule.
- **Delete entities**: Removes an entity which was inserted in the rule.

Hint: The position of each rule can be changed simply clicking and dragging it to the desired new position.

Policy: This option allows the edition of name and color, in order to change it simply click on the icon ***Policy***.

Adding and removing entities and services in the rule.

To add an entity in one of these fields you may proceed in two ways:

1. Select the entity to be added, and click on it in the *entities table* and drag it to the selected field. The ***Inset*** and ***Delete*** keys can add or remove the entities.
2. Right-click on the field where you wish to add the entities, a list of entities will be displayed.

    1. Double-click on the entity will open an editing box.

To remove an entity of one these fields, may proceed as follows:

1. Right-click on the field where the entity which you want to delete is. A list of entities will be displayed with a ***Delete*** option.
2. You can use the ***Delete Entities*** option to delete multiple entities at once.

In the rules creation when the entity is selected, you shall observe the source and destination. If an IPv4 address is specified in the source, mandatorily an IPv4 must to be specified in the destination, and the same process for the IPv6.

Rules parameters:

Beside the basic specifications of a rule, source entities, destination entities and services, shall consider other configuration parameters:

Counter: Defines which *counter* will be used for the rule packet. The *option "none"* disables the packets accounting that fits in this rule. If a *counter* is chosen, the amount of bytes and packet embedded in this rule will be added to the chosen *counter*.

Pipe: Defines the *Pipe* that will be used to control the band for the rule. The option "*none"* disables the use of band control for this rule.

Action: This field defines what action will be taken for all the packets that fit in this rule. It consists of the following rules:

Accept: Authorize packets that fit in the rule, in order to allow them pass through the firewall.

Reject: Prevent the packets which fit in this rule to pass through the firewall. Therefore, an ICMP packet will be sent to the source hosts of packet saying that the destination is unreachable. This option does not work for some types of ICMP services, due to the protocol inherent feature.

Discards: Means that the packets which fit in this rule will not pass through the firewall, but no packet will be sent to the source host.

Log: Defines what types of actions will be performed by the system when a packet fits in the rule. It consists of several options that can be selected independently of one another. The possible values are:

Logs: If this option is selected, all the packets that fit in this rule will be registered in the system log.

Sends email: If this option is selected, an email will be sent every time that a packet fits in this rule (the email address configuration will be displayed in the chapter titled ***configuring the system actions***).

Executes program: Selecting this option, a program chosen by the administrator will be executed every time a packet fits in this rule (the program's name to be executed will be displayed in the chapter titled ***configuring system actions***).

Triggers alarm: Selecting this option, the firewall shows an alert window every time a packet fits in this rule. This alert window will be displayed in the host where the Remote Interface is opened, if the host allows a beep will be sent. In case the Remote Interface is not opened, no message will be displayed and this option will be ignored.

Sends SNMP trap: Selecting this option, a Trap SNMP will be sent to each packet that fits in this rule (the parameters for the traps sending configuration will be displayed in the chapter titled ***configuring system actions)***.

For the TCP protocol, only the actions defined in the rule for the packet of connection opening will be performed. For the UDP protocol, all the packets that have been sent by the client host and if they fit in the rule (except the response packet) will trigger the performance of actions.

Time: Defines the time and days of the week which the rule will be applicable. The lines represent the week days and columns represent the time. In case you wish to make rule applicable in a specific time, the check box must to be checked, otherwise let it unchecked.

In order to facilitate the *Time* configuration, you can left click on the check box and drag it around, keeping it pressed. This way the tab will be modified as you move the mouse.

Validity Period: Allows registering two dates that delimit a period.

Comment: Add a comment about the rule. It is very useful in the documentation and maintenance of the information about the rule utility.

Verifying rules

The verifying rule is made through the icon ◉, or automatically, when the user apply the rules in the *apply* button in the ***Filtering rules window***.

Image 180 – Verifying rules *icons.*

The *Verifies Rules* button verifies the connection with the *Aker Control Center* and the eclipsed rules verification. *First* allows checking if there is any rule that prevent the user to connect to the firewall which is automatically configured.

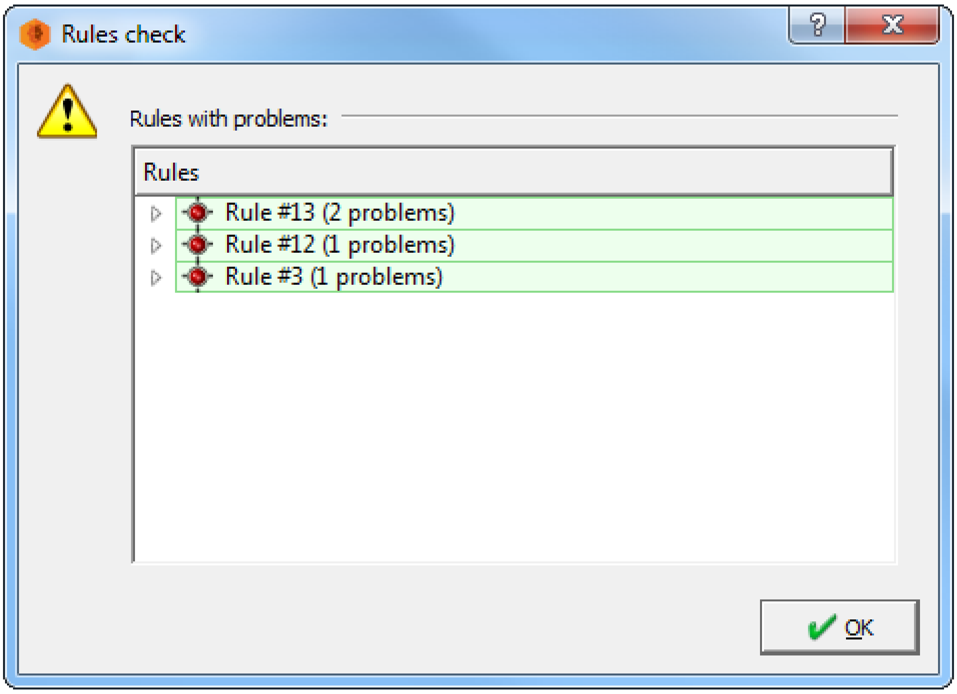
Example: The user IP is 10.0.0.1 and the firewall is 10.0.0.2 and the *control center* port is 1020. In case there is any rule saying to reject the packet origins 10.0.0.1 and packets destination 10.0.0.2 on port 1020, in case this rule is applied, the user shall not be able to connect to this firewall. Is a mechanism to prevent the user from shutdown your own connection access in the firewall.

Second is the "*eclipse*", this verification is necessary when the 1st rule encloses completely to the 2nd rule, preventing the 2nd rule to be reached.

Example: The 1st rule is 0.0.0.0 (any source), destination 0.0.0.0 (any destination) and all TCP 7 ports.

The 2nd rule is 10.0.0.1, and destination 10.0.0.2 is TCP7 port. The first rule does everything which the 2nd rule does, so the 2nd rule will never be reached, because the 1st rule will be processed first and will not let the other rule to be reached.

Note: All the rules are verified, they are rules that already exist, in other words rules that already have been defined.



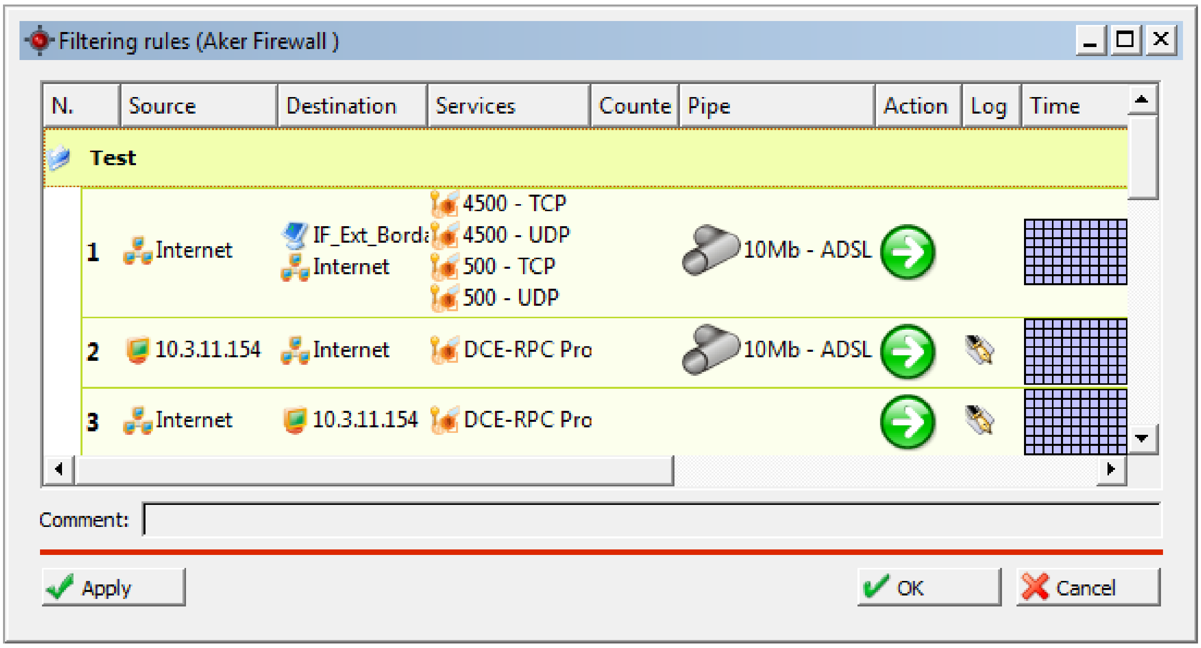
Rules check
Rules with problems:
Rules
OK

Rule #13 (2 problems)
Rule #12 (1 problems)
Rule #3 (1 problems)

Image 181 – Rules check.

The use of Pipe in the Filtering rule in Aker Firewall

The administrator can set Quality of service (QoS) for each rule type. In the Image below, was created a *Pipe* of 10Mb- ADSL and applied in rules 1 and 2. The server "SMTP_mail" has priority in traffic because the priority for it in the pipe is "very high".

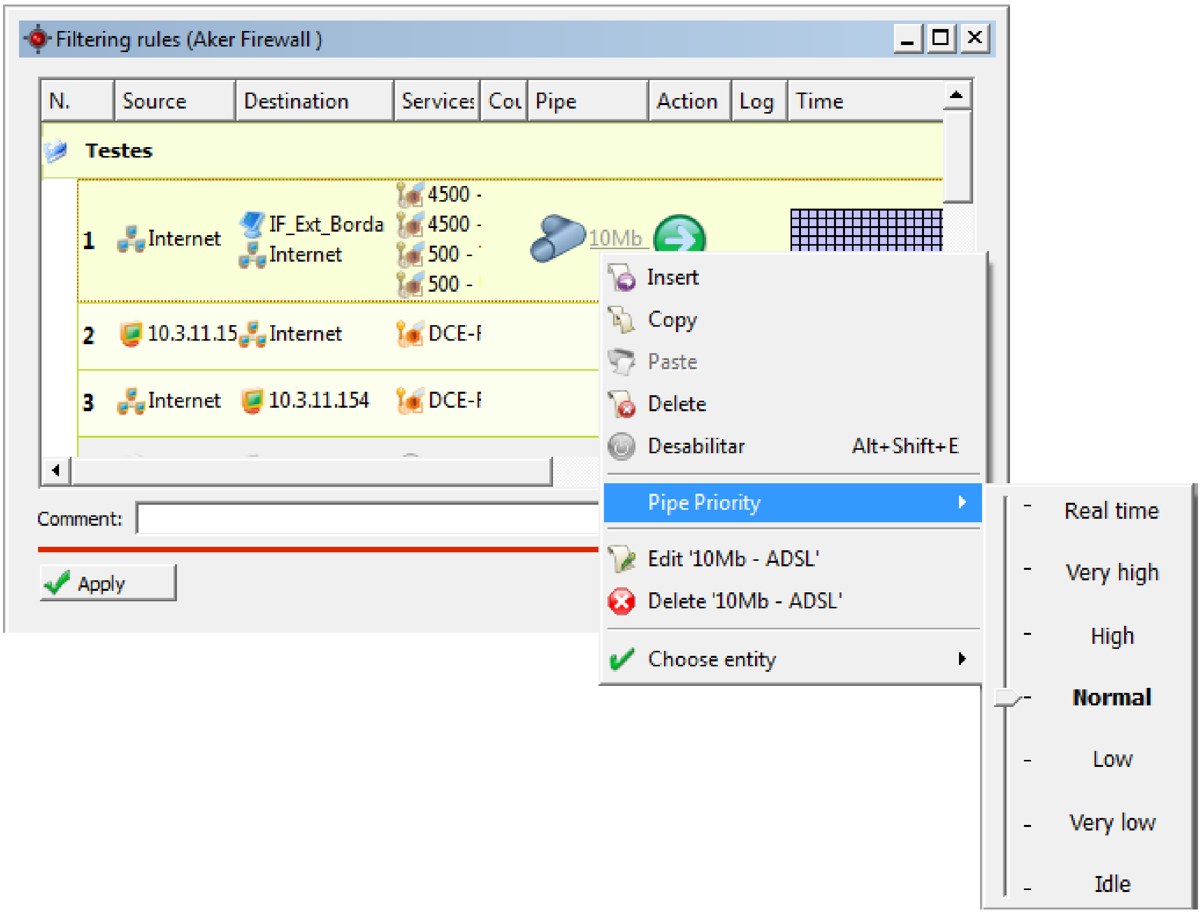


Filtering rules (Aker Firewall)
Comment:
Apply
OK
Cancel

N.	Source	Destination	Services	Counte	Pipe	Action	Log	Time
Test								
1	Internet	IF_Ext_Bord Internet	4500 - TCP 4500 - UDP 500 - TCP 500 - UDP		10Mb - ADSL	→		▦
2	10.3.11.154	Internet	DCE-RPC Pro		10Mb - ADSL	→	✎	▦
3	Internet	10.3.11.154	DCE-RPC Pro			→	✎	▦

Image 182 – Filtering rules (Example of pipe 10Mb – ADSL).

For *pipe priority settings*, just right-click on the Pipe entity and choose the priority by the sliding button. As the example below:



Filtering rules (Aker Firewall)
Insert
Copy
Paste
Delete
Desabilitar Alt+Shift+E
Pipe Priority
Edit '10Mb - ADSL'
Delete '10Mb - ADSL'
Choose entity
Real time
Very high
High
Normal
Low
Very low
Idle
Comment:
Apply

N.	Source	Destination	Services	Cou	Pipe	Action	Log	Time
Testes								
1	Internet	IF_Ext_Borda Internet	4500 - 4500 - 500 - 500 -		10Mb			
2	10.3.11.15	Internet	DCE-I					
3	Internet	10.3.11.154	DCE-I					

Image 183 – Pipe priority settings.

7.3. Working with the filtering Polices

This resource allows the firewall administrator to make a rule grouping within a survey of flow which occurs among its sub networks.

To illustrate, let us assume that the administrator has a firewall placed between the Intranet, DMZ and Internet, as the Image below:

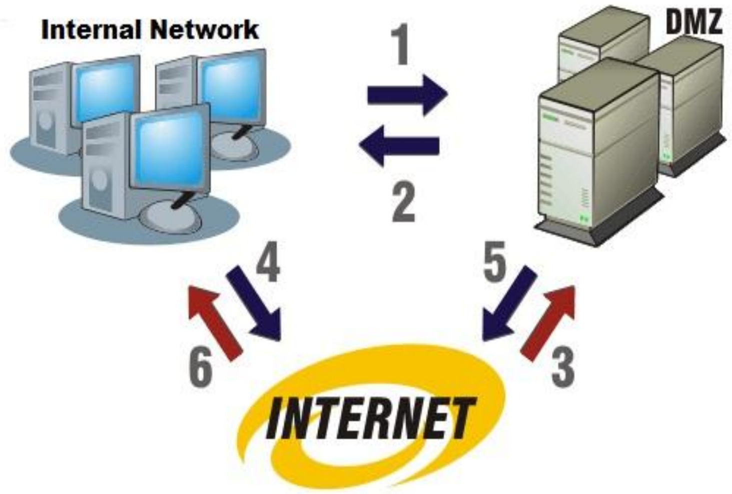
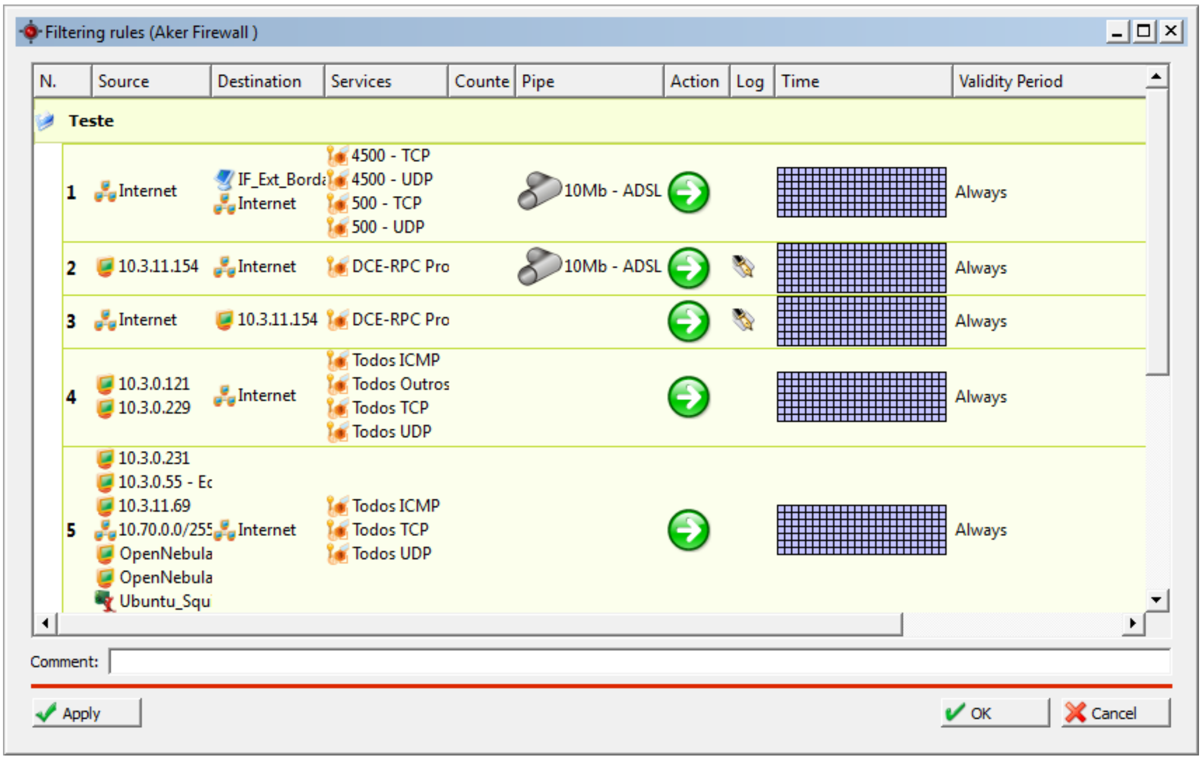


Image 184 – Example of how to work with filtering policies.

You can check the possible data flow that may occur among these networks. For each flow has been given a numbering and with this we can conclude that the flows with the higher numbers (5 and 6) are considered the most insecure, because they involve the internet access to DMZ and Intranets, respectively.

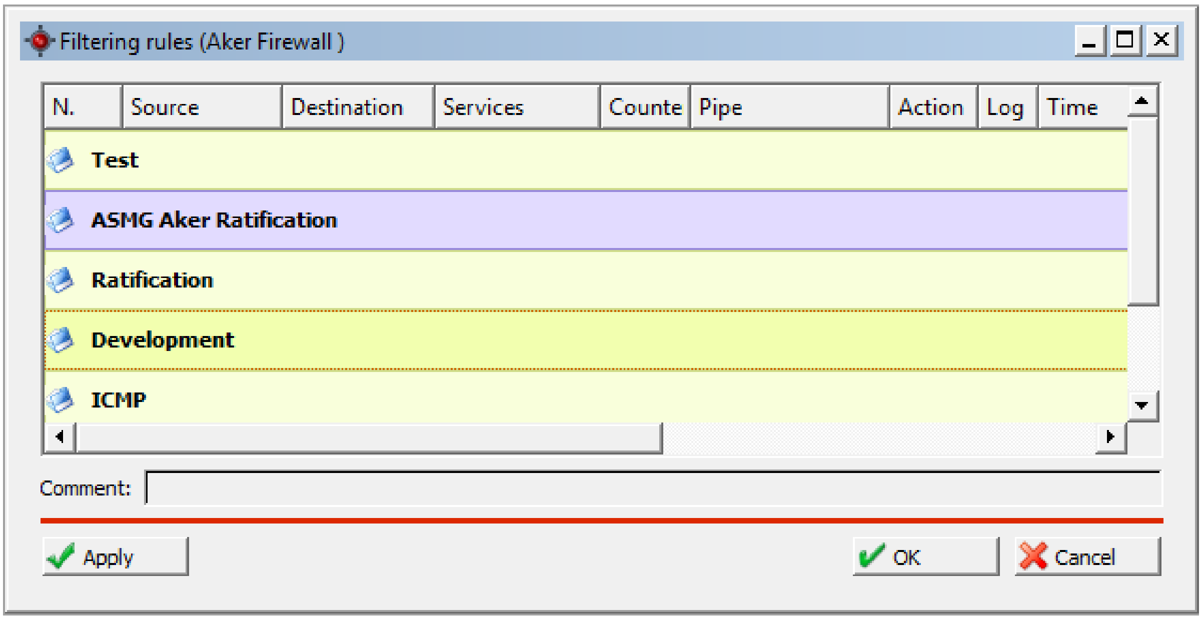
These flows for the firewall will be deployed in filtering rules, and then we could have the following rules:


Filtering rules (Aker Firewall)
Apply
OK
Cancel

N.	Source	Destination	Services	Counte	Pipe	Action	Log	Time	Validity Period
Teste									
1	Internet	IF_Ext_Bord Internet	4500 - TCP 4500 - UDP 500 - TCP 500 - UDP		10Mb - ADSL	→		▦	Always
2	10.3.11.154	Internet	DCE-RPC Pro		10Mb - ADSL	→	✎	▦	Always
3	Internet	10.3.11.154	DCE-RPC Pro			→	✎	▦	Always
4	10.3.0.121 10.3.0.229	Internet	Todos ICMP Todos Outros Todos TCP Todos UDP			→		▦	Always
5	10.3.0.231 10.3.0.55 - Ec 10.3.11.69 10.70.0.0/255 OpenNebula OpenNebula Ubuntu_Squ	Internet	Todos ICMP Todos TCP Todos UDP			→		▦	Always

Comment:

Image 185 – Examples of filtering rules


Filtering rules (Aker Firewall)
Apply
OK
Cancel

N.	Source	Destination	Services	Counte	Pipe	Action	Log	Time
Test								
ASMG Aker Ratification								
Ratification								
Development								
ICMP								

Comment:

Image 186 – Filtering rules Interface

In order to create new “policies", simply click on the toolbar icon “Policy”

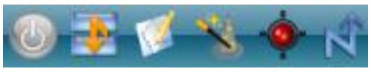


Image 187 – Icon bar (Policy).

The Image below shows the deployment of the policy rules. Just double click on the line to display the rules that contain in it:

Image 188- Display filtering rules

If you disable a policy, all the rules within this policy will be disabled as well.

7.4. Using the text interface

The use of Text Interface in the filtering rules configuration brings a difficulty created by the large amount of parameters that must to be passed from the command line.

It is not configure the *time* nor specify comments for the rules through the Text Interface. And also is not possible to specify more than one entity for the source or destination of rule. All the rules added by this interface are considered applicable at all the week times.

Program location: /aker/bin/firewall/fwrule.

Syntax:

```
Usage: fwrule [help | show]
   fwrule [enable | disable | remove] <pos>
   fwrule add <pos> <source> <destination>
                    <accept | reject | discard>
           [pipe <pipe> <weight>] [counter <counter>]
           [log] [mail] [trap] [program] [alert]
           [encrypted | user ] [<service> ...]
```

Program help:

```
Aker Firewall –
fwrule – Configure the stateful inspection rules table
Usage: fwrule [help | show]
    fwrule [enable | disable | remove] <pos>
    fwrule adds <pos> <source> <destination>
           <accept | reject | discard>
           [pipe <pipe> <weight>] [counter <counter>]
           [log] [mail] [trap] [program] [alert]
           [encrypted | user ] [<service> ...]

   show     = show all the entries of the rule table
   add      = adds a new filtering rule
```

enable *= enables a disabled filtering rule*
disable *= disables an existing filtering rule*
remove ***=*** *removes an existing rule*
help *= shows this message*

To add:

pos *= position where you add a new rule in the table.*
accept *= the rule accepts the connections that fits in it.*
reject *= the rule rejects the connections that fits in it and sends ICMP destination unreachable packet to the source host*
discard *= the rule discards received packets (does not sent ICMP packet)*
pipe *= causes the traffic that fits in this rule be directed to the "pipe" indicated with the relative weight given by :*
counter *= causes the traffic that fits in this rule be added to the specific counter entity*
weight *= "idle", "m_low" (very low), "low", "normal", "high", "m_high" (very high) or "tr" (real time)*
log *= logs the packets which fits in the rule*
mail *= sends an email to each packet that which in the rule*
trap *= generates SNMP trap for each packet which fits in the rule*
program *= runs a program for each packet which fits in this rule*
alert *= opens an alert window for each packet which fits in this rule*
encrypted *= indicates that the rule is valid only if the packets are encrypted*
user *= indicates that the rule is valid only if the packets are encrypted and the user has previously authenticated at the firewall. This condition can only be met by connections from encryption client*
service *= lists the services names for the new rule*

To enable / disable / remove:

pos = number of rule to be enabled, disabled or removed

Example 1: (visualizing filtering rules)

```
#/aker/bin/firewall/fwrule show

Rule 01
--------
Source      : Internet
Destination   : firewall      cache
Action       : Discards
```

```
Log        : Logs Trap Alert
Services  : All_tcp       all_udp
                                  all_icmp
Rule 02
--------
Source     : cache                firewall
Destination     : Internet
Action        : Accepts
Log        : Logs
Services    : http                 ftp

Rule 03
--------
Source     : Internet
Destination     : Mail server
Action       : Accepts
Log        : Logs
Services    : smtp

Rule 04
--------
Source     : External Enterprises
Destination     : Aker
Action        : Accepts
Log         : Logs
Services     : smtp
```

Example 2: (Removing the forth filtering rule)

```
#/aker/bin/firewall/fwrule remove 4

Rule 4 removed
```

Example 3: (adding a new rule at the end of the table)

```
#/aker/bin/firewall/fwrule add in the end Internet "Mail server" accepts smtp log
Rule added in position 4
```

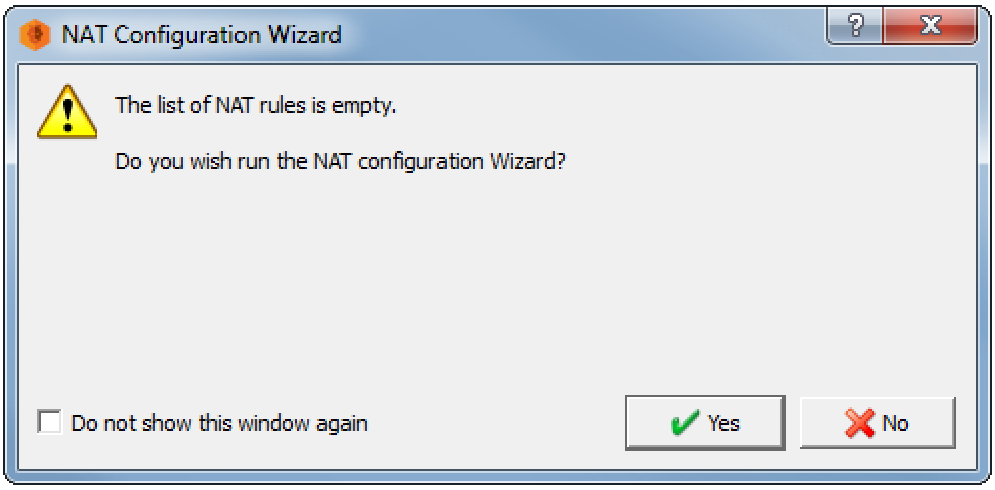
The Internet entities and Mail server, as the SMTP service must have been previously registered in the system. For more information about how to register entities in Aker Firewall, for more information see the chapter ***Registering Entities***.

The use of "" (quotation marks) around the entity name to be in the rule is mandatory when it contains spaces.

7.5. Using the Filtering rules wizard.

The *rules wizard* can be activated through the menu or taskbar. In case the number of rules is too small the wizard itself will fire automatically.

1 – Using the *rules wizard*. The window below will be displayed when a small number of rules are detected.



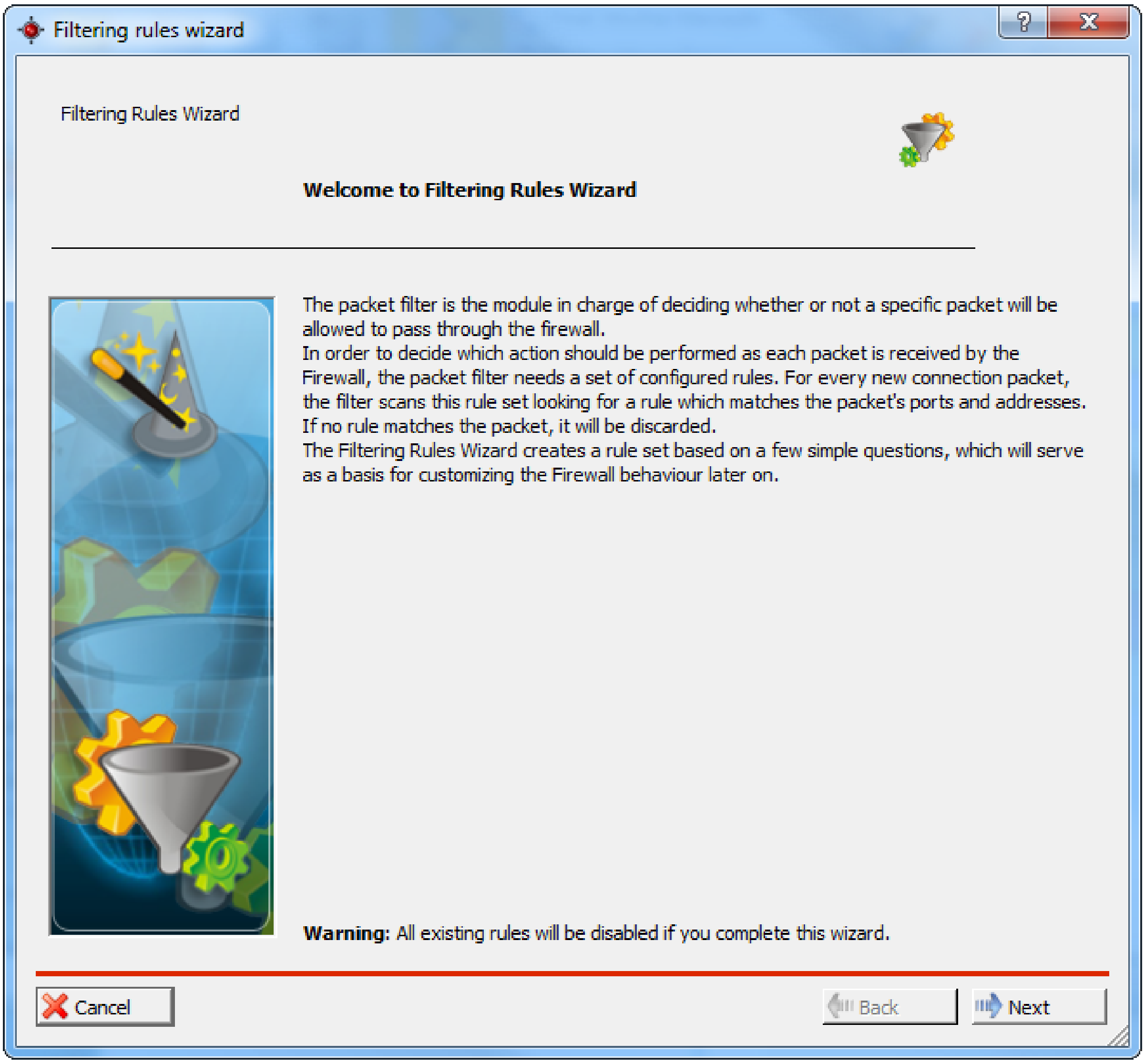
The list of NAT rules is empty.

Do you wish run the NAT configuration Wizard?

☐ Do not show this window again

Image 189 – Filtering rules wizard

2 – Home screen with the necessary explanations.



Filtering Rules Wizard

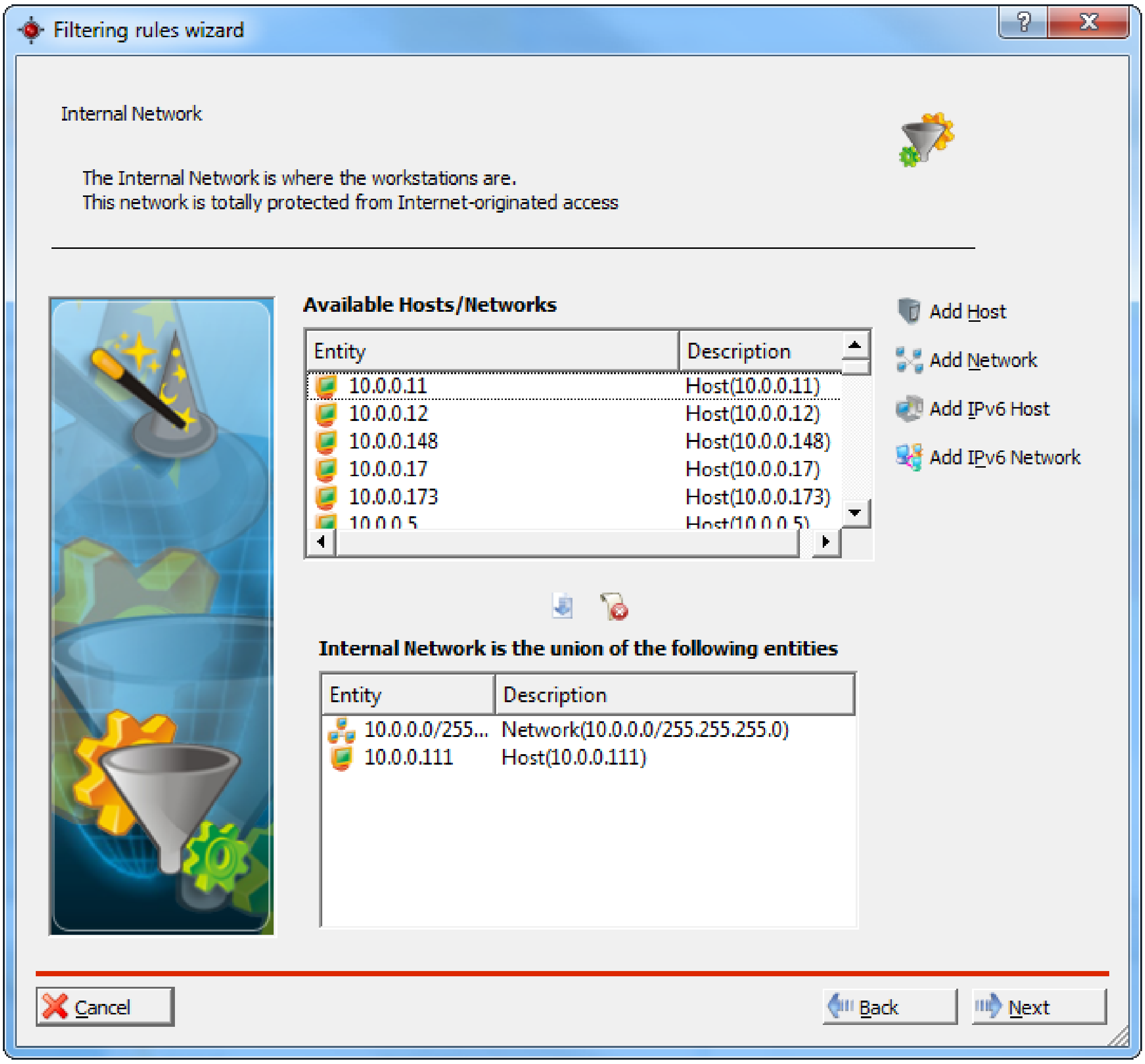
Welcome to Filtering Rules Wizard

The packet filter is the module in charge of deciding whether or not a specific packet will be allowed to pass through the firewall.
In order to decide which action should be performed as each packet is received by the Firewall, the packet filter needs a set of configured rules. For every new connection packet, the filter scans this rule set looking for a rule which matches the packet's ports and addresses.
If no rule matches the packet, it will be discarded.
The Filtering Rules Wizard creates a rule set based on a few simple questions, which will serve as a basis for customizing the Firewall behaviour later on.

Warning: All existing rules will be disabled if you complete this wizard.

Image190 – Filtering rules wizard welcome message

3 – Choose the Intranet in the initial configuration.



Filtering rules wizard

Internal Network

The Internal Network is where the workstations are.
This network is totally protected from Internet-originated access

Available Hosts/Networks

Entity	Description
10.0.0.11	Host(10.0.0.11)
10.0.0.12	Host(10.0.0.12)
10.0.0.148	Host(10.0.0.148)
10.0.0.17	Host(10.0.0.17)
10.0.0.173	Host(10.0.0.173)
10.0.0.5	Host(10.0.0.5)

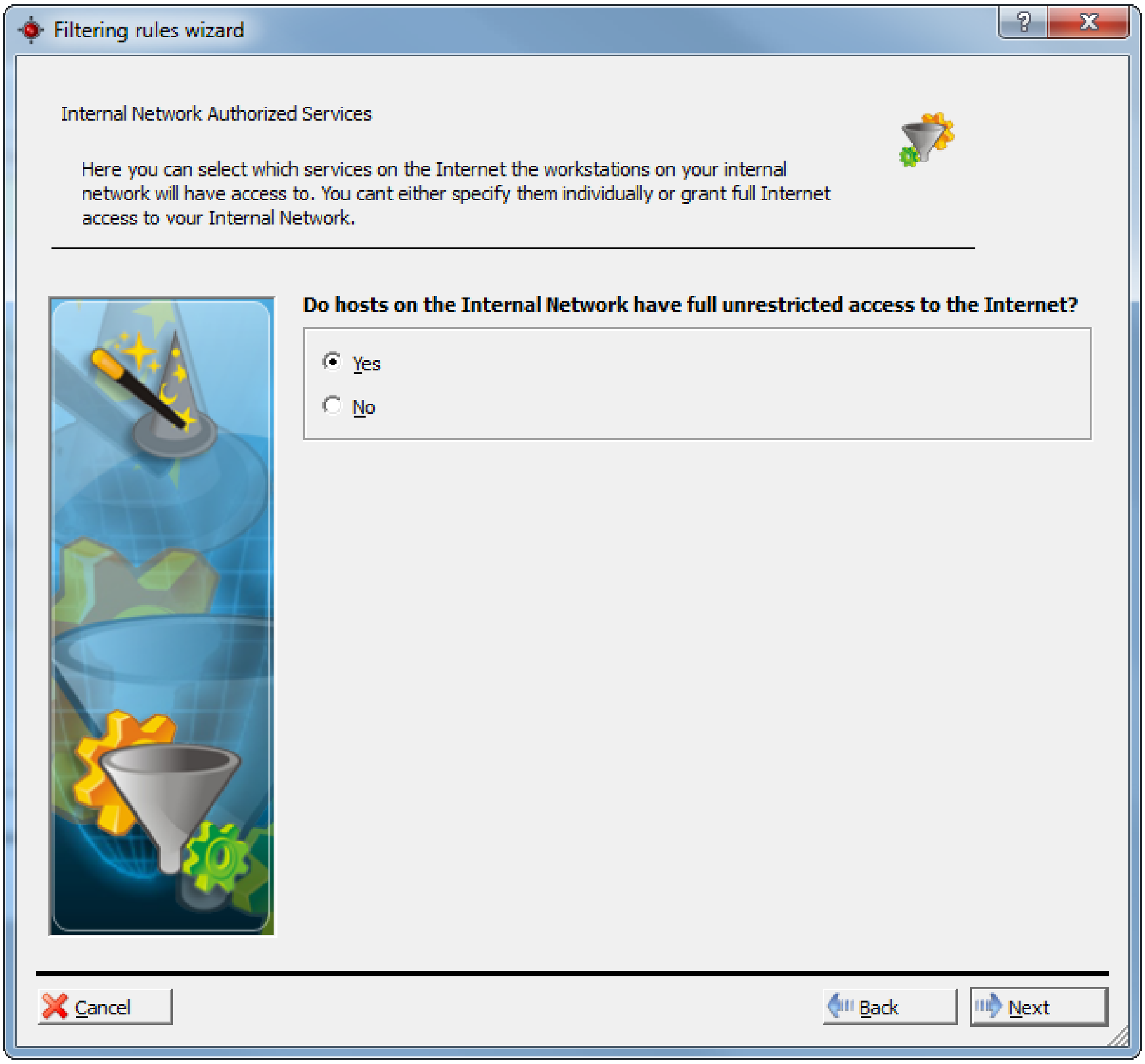
Internal Network is the union of the following entities

Entity	Description
10.0.0.0/255...	Network(10.0.0.0/255.255.255.0)
10.0.0.111	Host(10.0.0.111)

Add Host
Add Network
Add IPv6 Host
Add IPv6 Network
Cancel
Back
Next

Image 191 – Choosing the Intranet in the initial configuration.

4 – Information necessary to know if hosts will have unrestricted Internet access.



Internal Network Authorized Services

Here you can select which services on the Internet the workstations on your internal network will have access to. You cant either specify them individually or grant full Internet access to vour Internal Network.

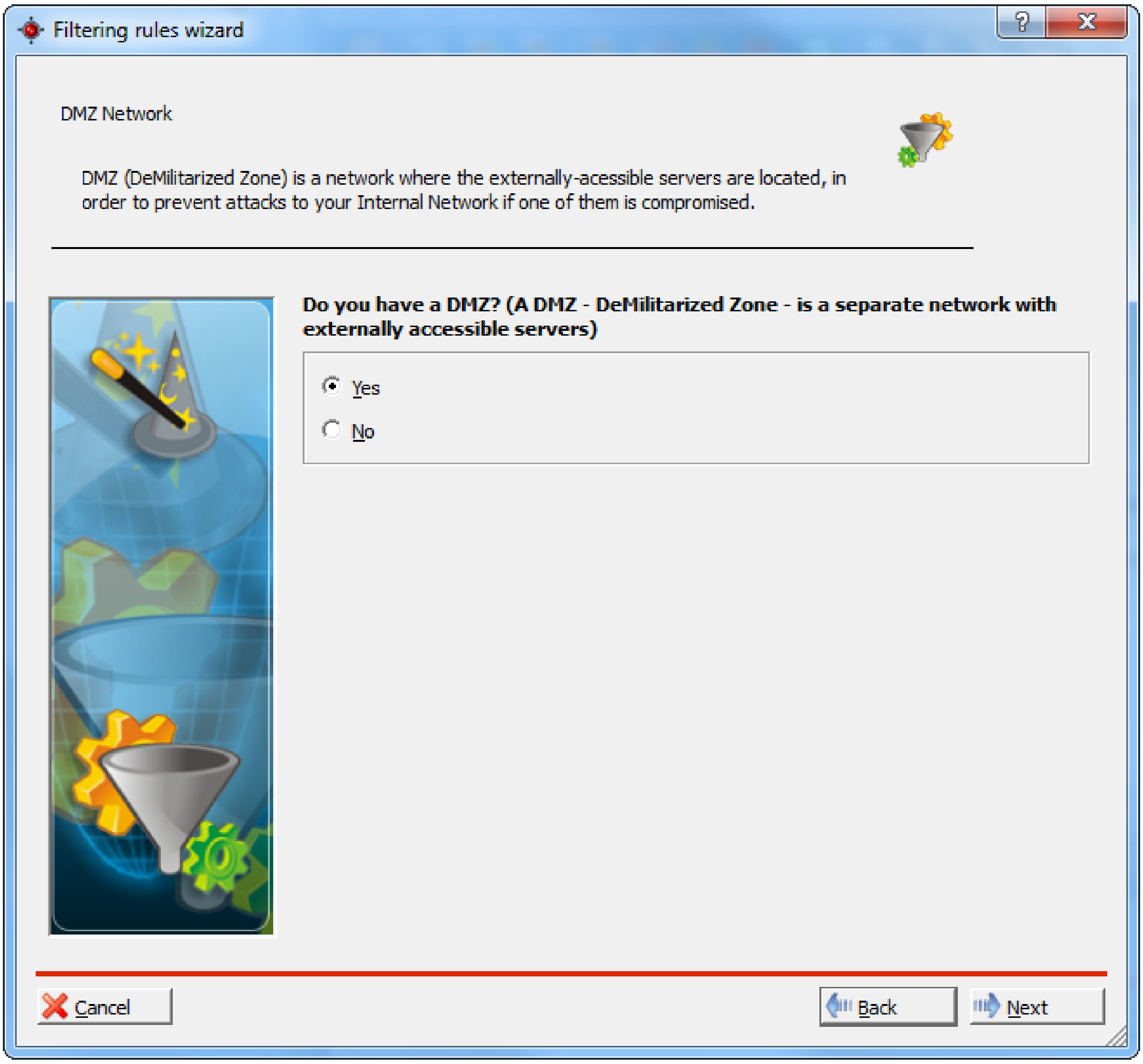
Do hosts on the Internal Network have full unrestricted access to the Internet?

● Yes

○ No

Image 192 – Access screen to choose restricted access or not to the internet

5 – DMZ configuration.



DMZ Network

DMZ (DeMilitarized Zone) is a network where the externally-acessible servers are located, in order to prevent attacks to your Internal Network if one of them is compromised.

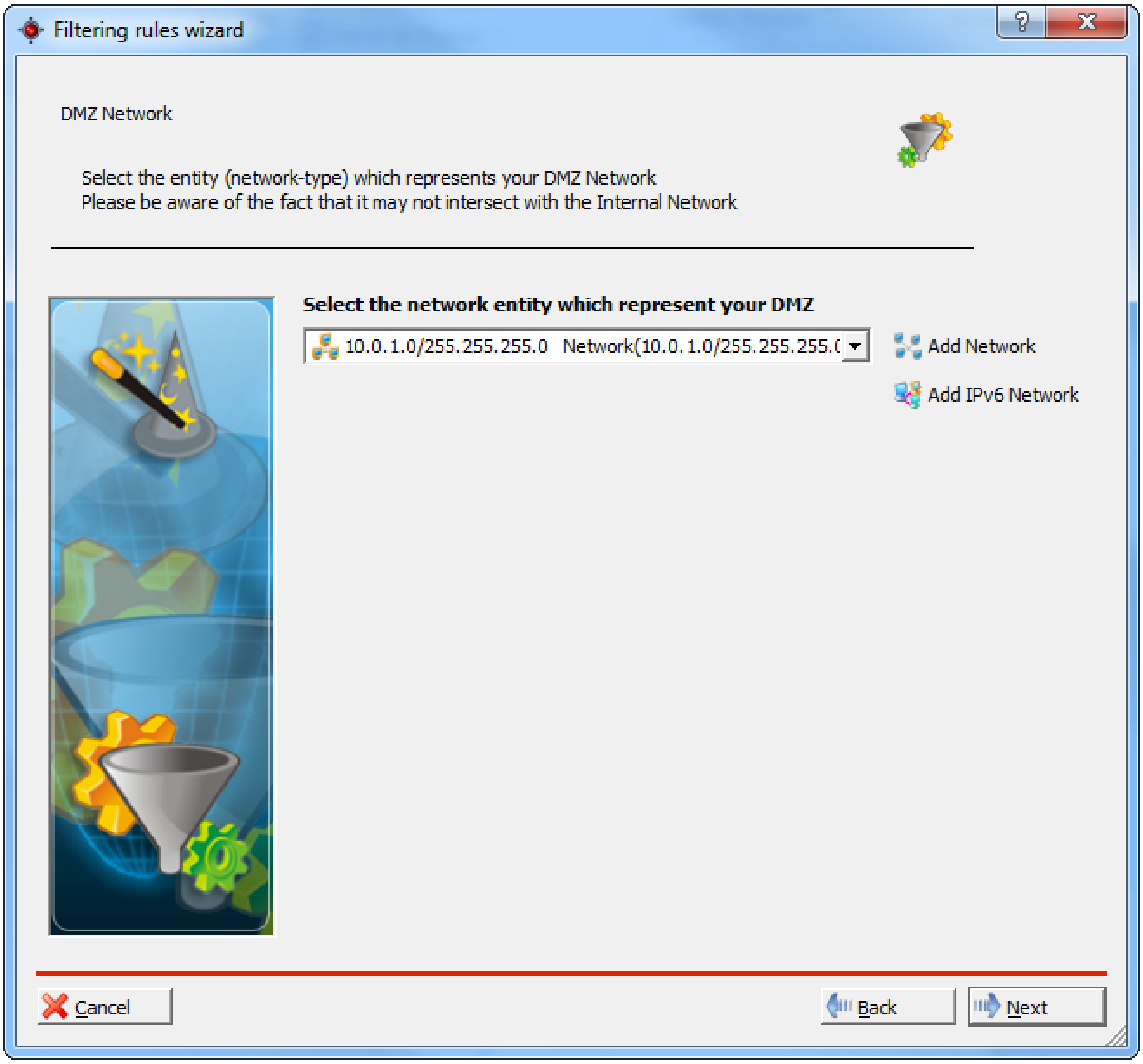
Do you have a DMZ? (A DMZ - DeMilitarized Zone - is a separate network with externally accessible servers)

● Yes

○ No

Image 193 –Choose whether there is or not a DMZ

6 – Choosing DMZ entity.


Filtering rules wizard

DMZ Network

Select the entity (network-type) which represents your DMZ Network
Please be aware of the fact that it may not intersect with the Internal Network

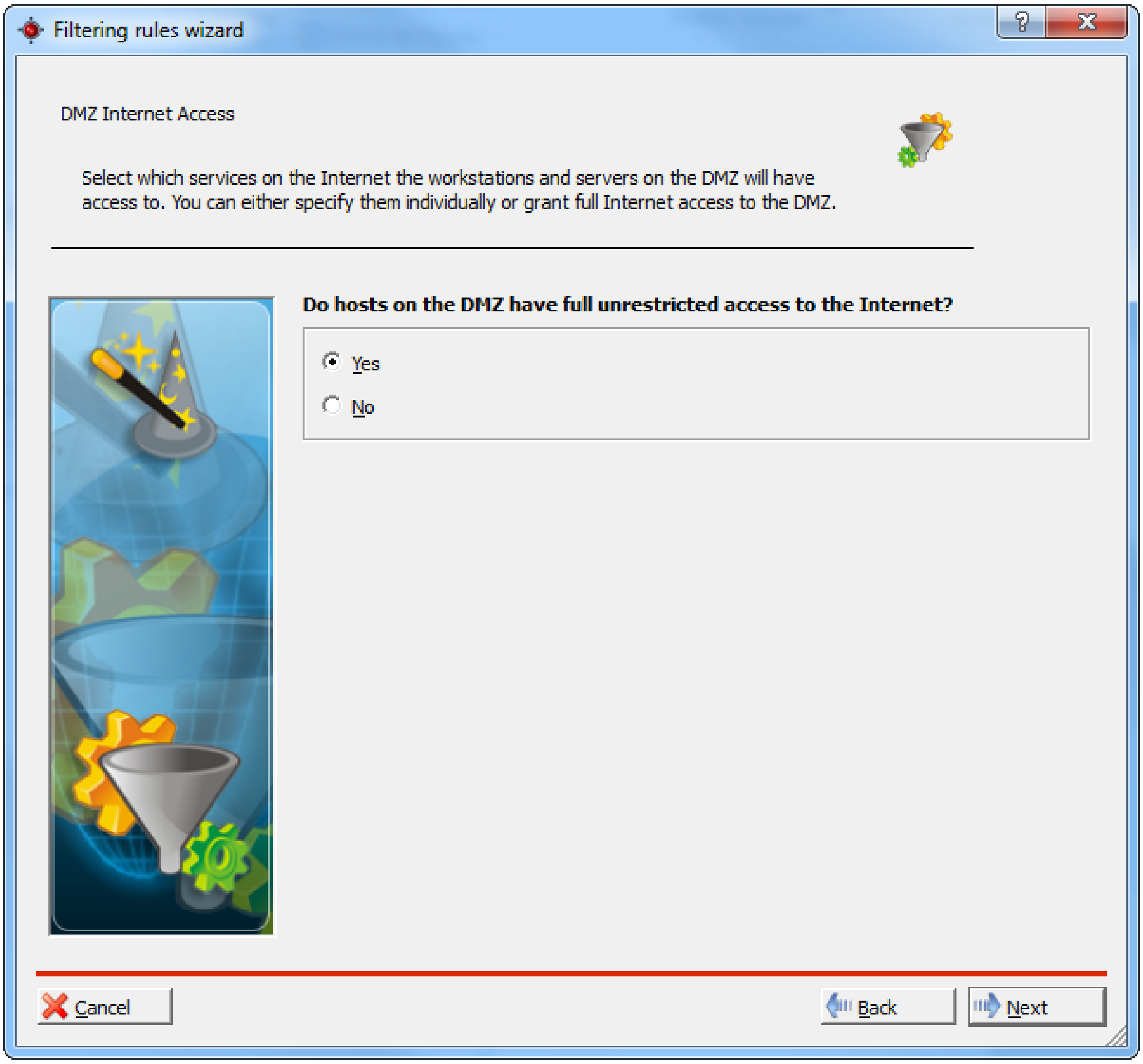
Select the network entity which represent your DMZ

10.0.1.0/255.255.255.0 Network(10.0.1.0/255.255.255.0

Add Network
Add IPv6 Network
Cancel
Back
Next

Image 194 – DMZ entity choice

7 – Inform if the DMZ will have unrestricted access to the Internet.



DMZ Internet Access

Select which services on the Internet the workstations and servers on the DMZ will have access to. You can either specify them individually or grant full Internet access to the DMZ.

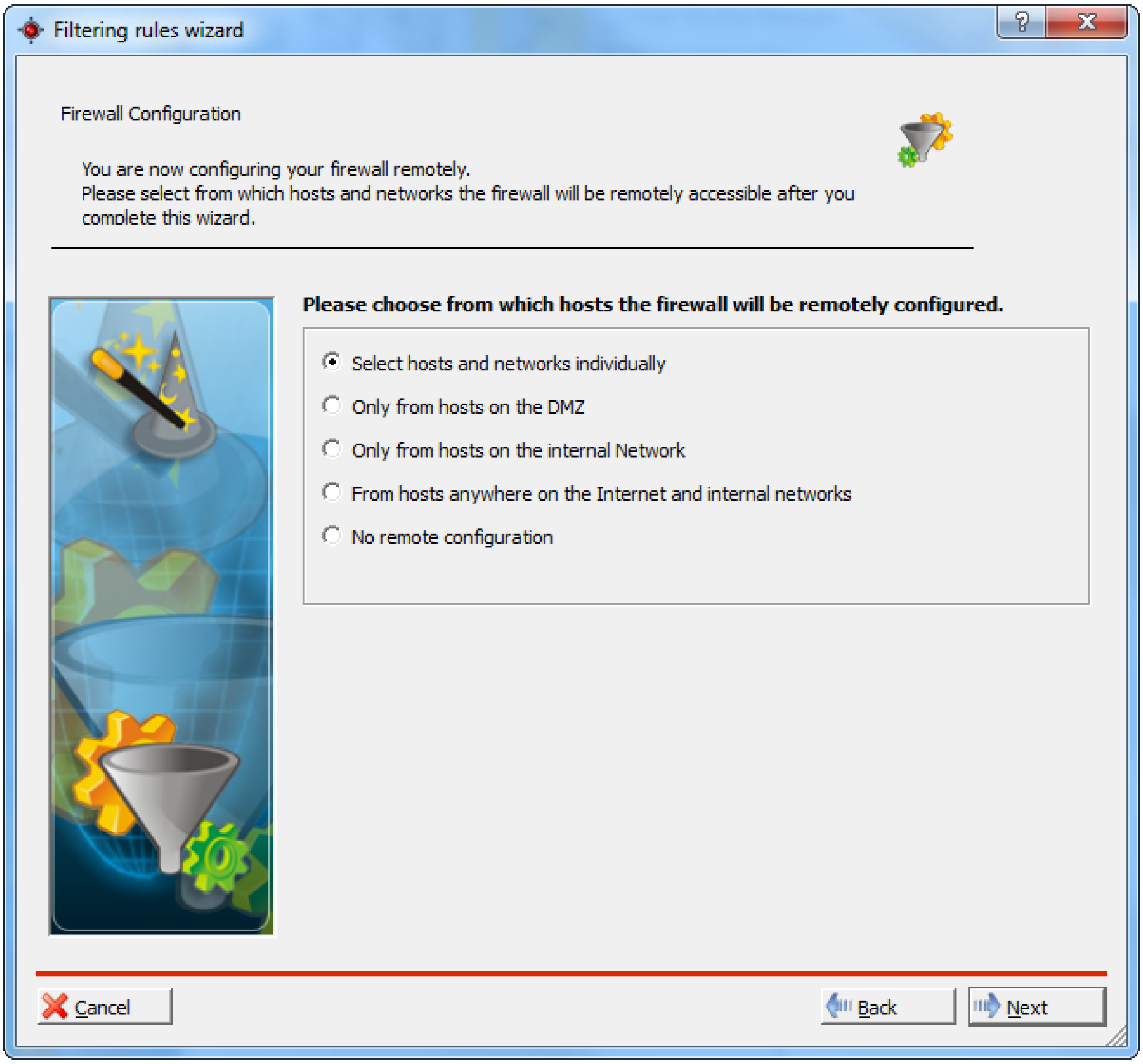
Do hosts on the DMZ have full unrestricted access to the Internet?

● Yes

○ No

Image 195 – DMZ hosts (restrict access or not to the Internet)

8 – Firewall administration. Informs who shall have administration access.



Firewall Configuration

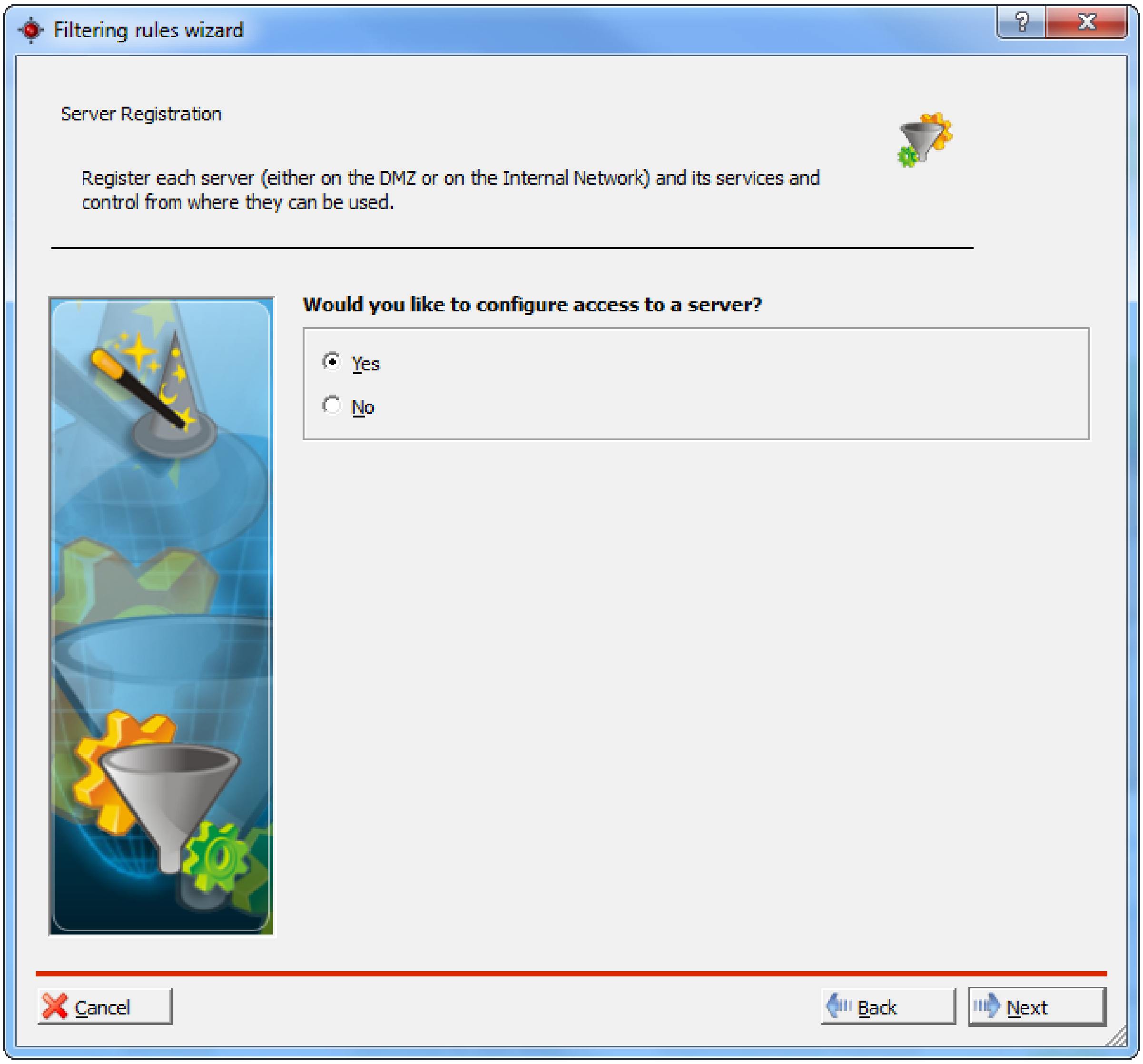
You are now configuring your firewall remotely.
Please select from which hosts and networks the firewall will be remotely accessible after you complete this wizard.

Please choose from which hosts the firewall will be remotely configured.

- ● Select hosts and networks individually
- ○ Only from hosts on the DMZ
- ○ Only from hosts on the internal Network
- ○ From hosts anywhere on the Internet and internal networks
- ○ No remote configuration

Image 196 – Firewall configuration

9- Individual register to the DMZ server.



Filtering rules wizard

Server Registration

Register each server (either on the DMZ or on the Internal Network) and its services and control from where they can be used.

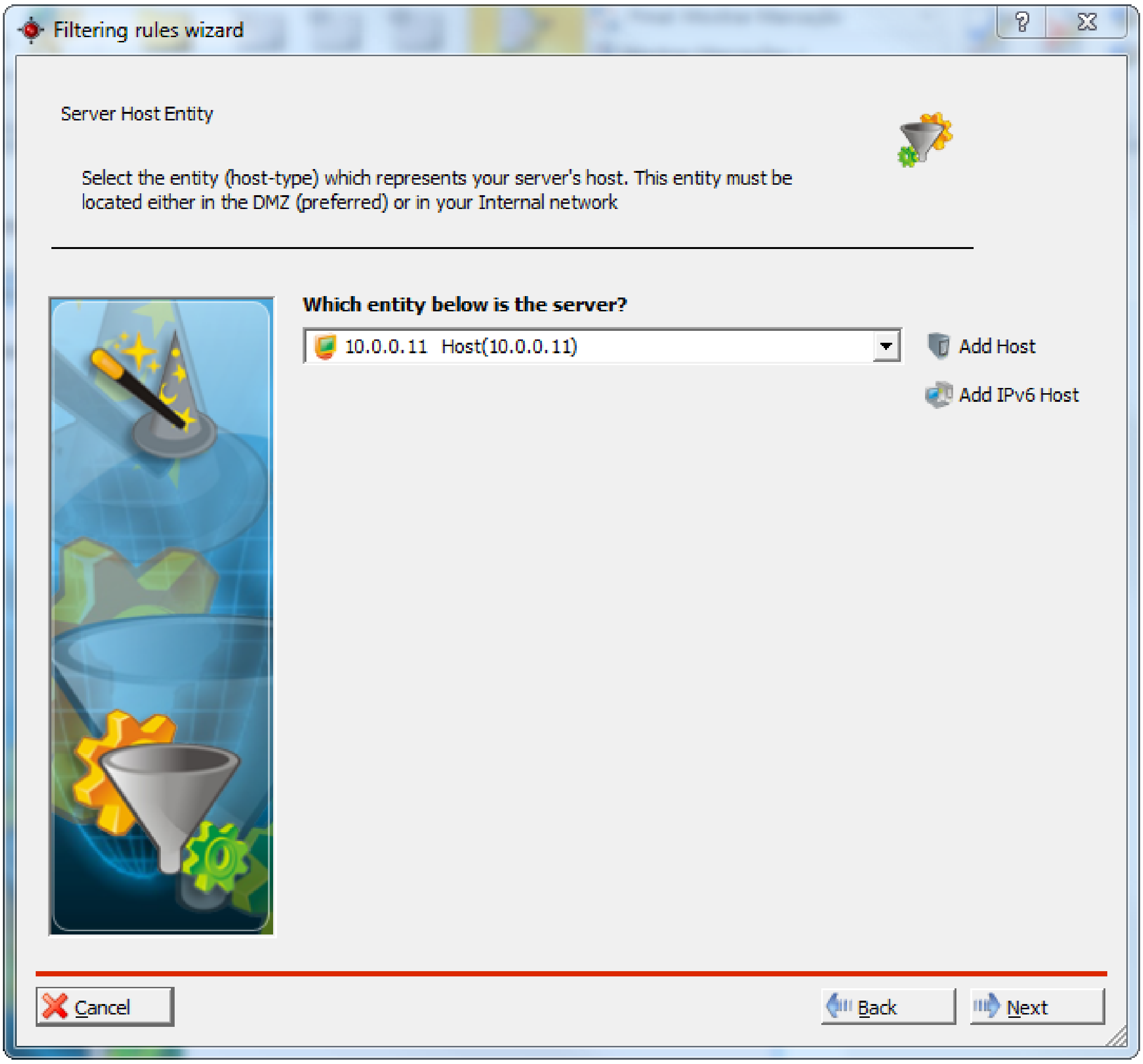
Would you like to configure access to a server?

● Yes
○ No

Cancel
Back
Next

Image 197 – Server Registration

10 – Specific server information to the DMZ.



Filtering rules wizard

Server Host Entity

Select the entity (host-type) which represents your server's host. This entity must be located either in the DMZ (preferred) or in your Internal network

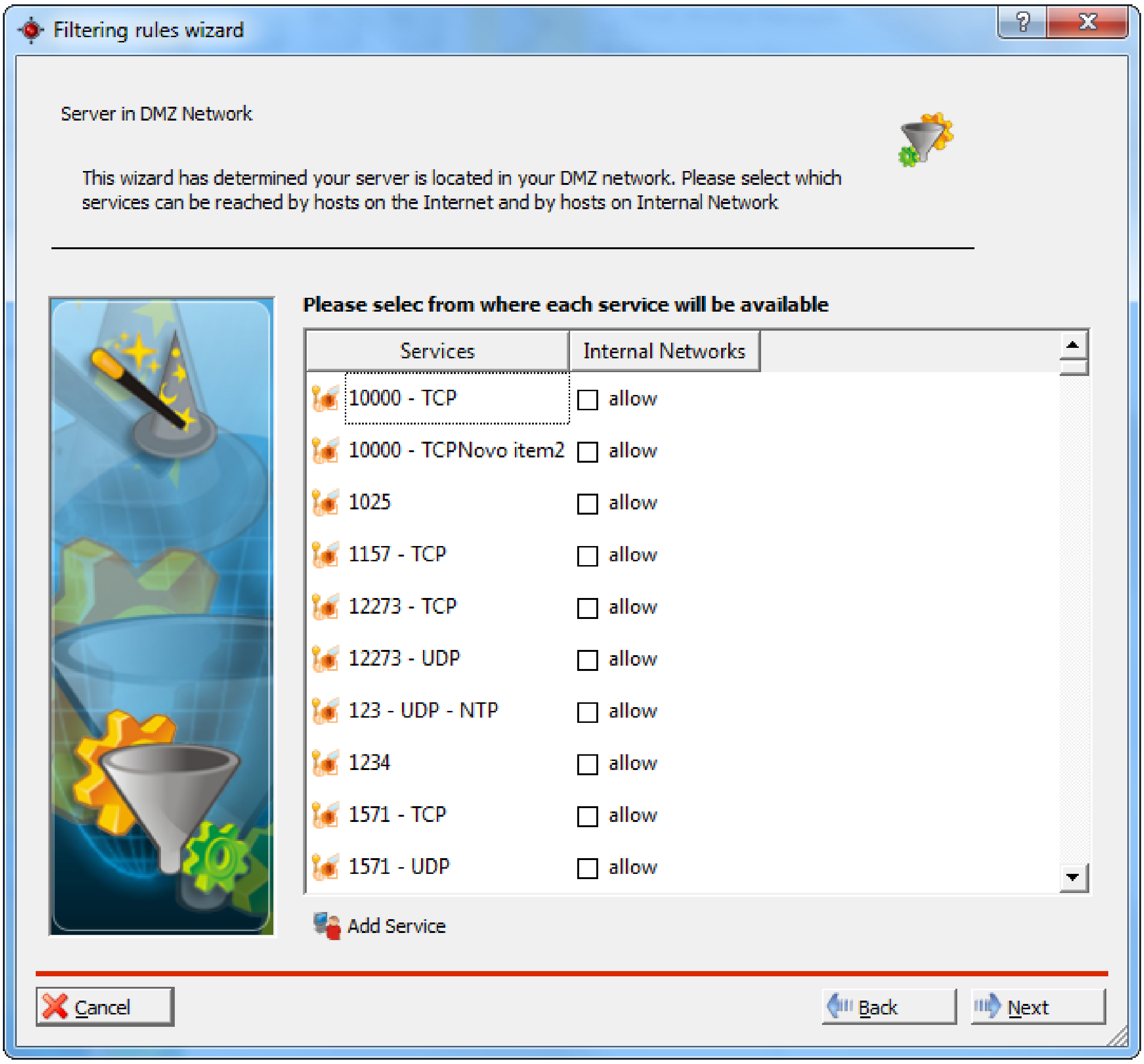
Which entity below is the server?

10.0.0.11 Host(10.0.0.11)

Add Host
Add IPv6 Host
Cancel
Back
Next

Image 198 – Choice of server entity

11 – Selection of server services for the DMZ.



Filtering rules wizard

Server in DMZ Network

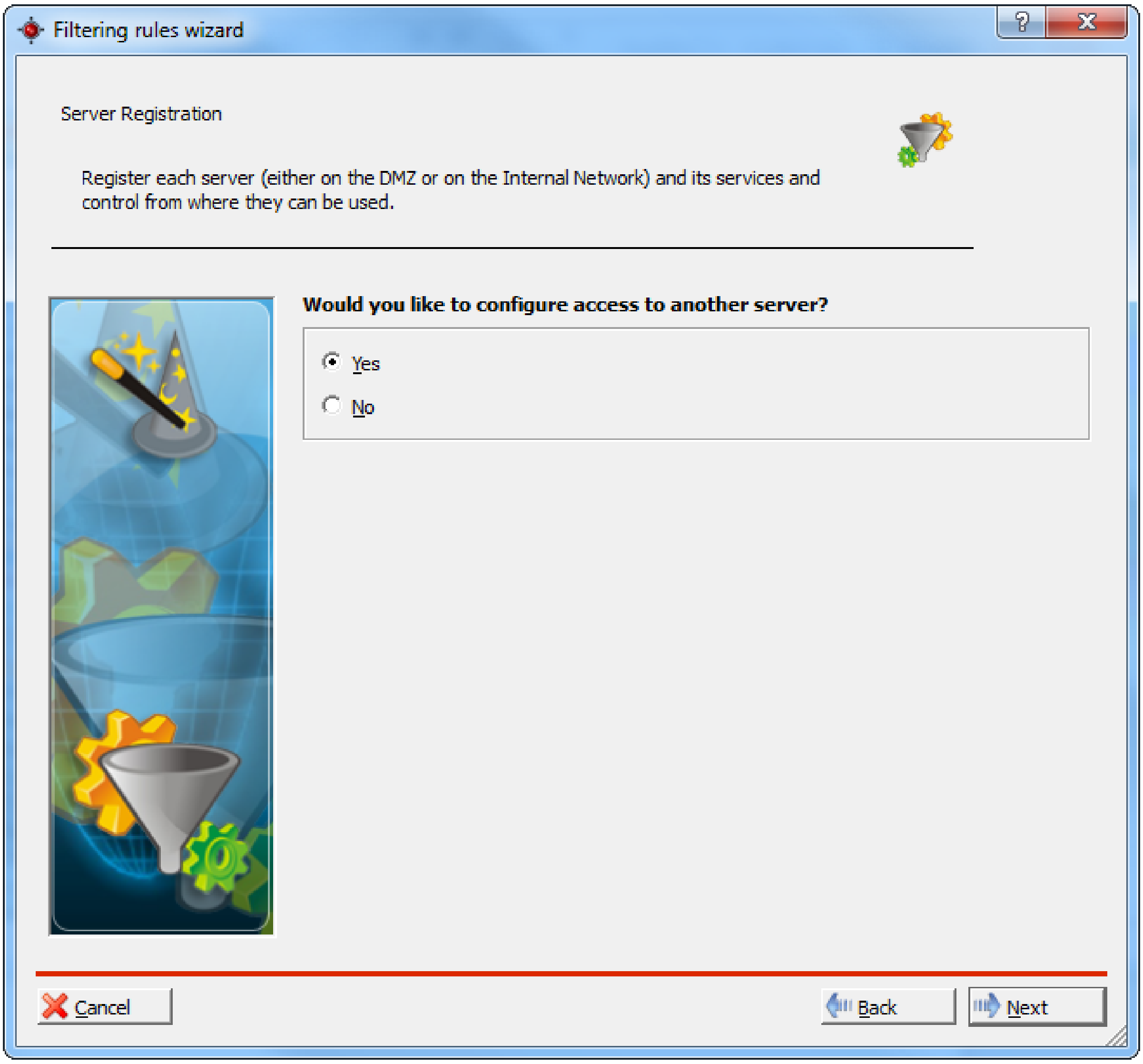
This wizard has determined your server is located in your DMZ network. Please select which services can be reached by hosts on the Internet and by hosts on Internal Network

Please selec from where each service will be available

Services	Internal Networks
10000 - TCP	☐ allow
10000 - TCPNovo item2	☐ allow
1025	☐ allow
1157 - TCP	☐ allow
12273 - TCP	☐ allow
12273 - UDP	☐ allow
123 - UDP - NTP	☐ allow
1234	☐ allow
1571 - TCP	☐ allow
1571 - UDP	☐ allow

Image 199 – Select the location where the DMZ will be available

12 – Question about configuring other server.



Filtering rules wizard

Server Registration

Register each server (either on the DMZ or on the Internal Network) and its services and control from where they can be used.

Would you like to configure access to another server?

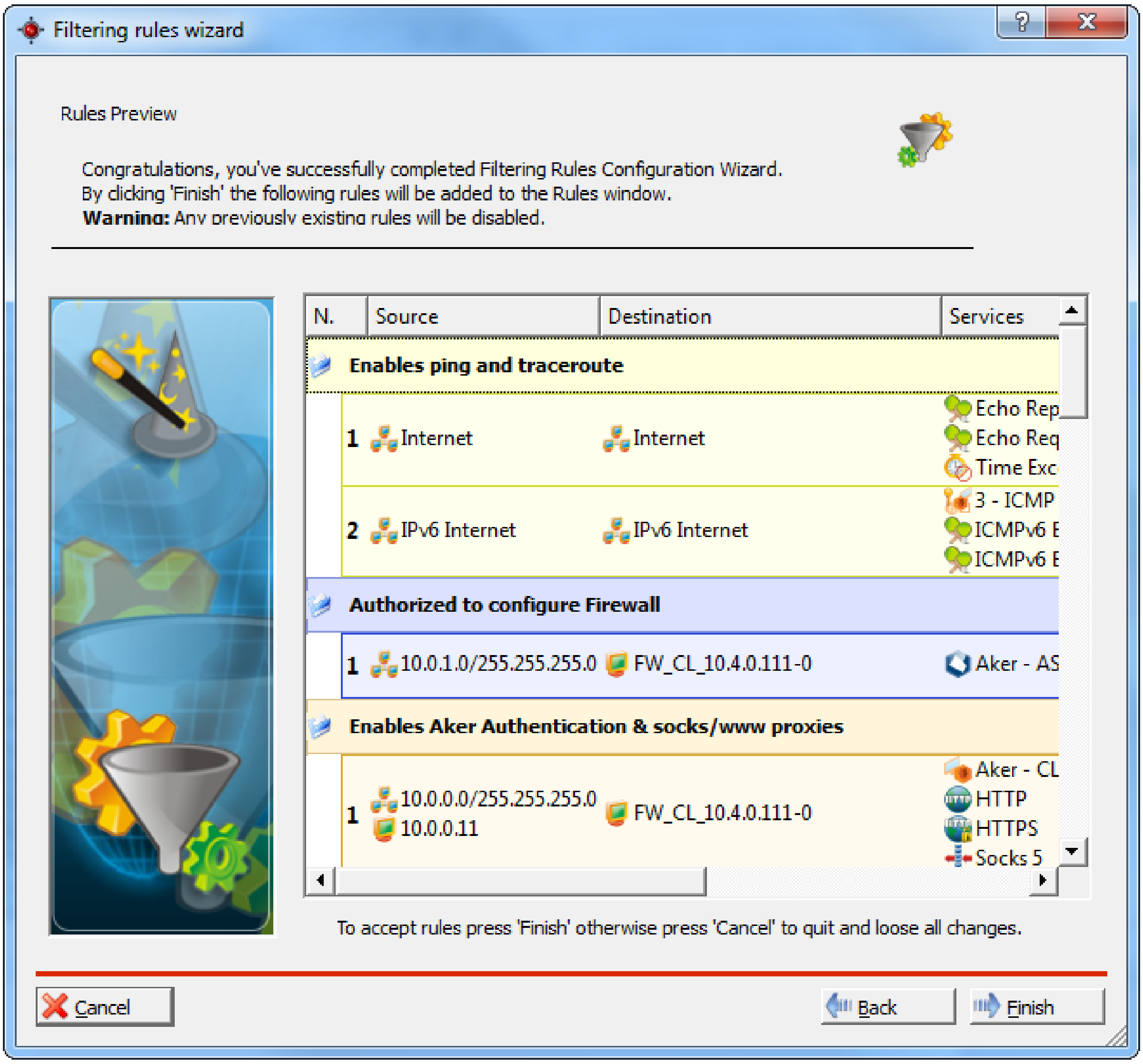
● Yes

○ No

Cancel
Back
Next

Image 200 – Choose to configure another server or not

13 – Final preview of the filtering rules wizard mounted by user.



Rules Preview

Congratulations, you've successfully completed Filtering Rules Configuration Wizard.
By clicking 'Finish' the following rules will be added to the Rules window.
Warning: Any previously existing rules will be disabled.

N.	Source	Destination	Services
Enables ping and traceroute			
1	Internet	Internet	Echo Rep Echo Req Time Exc
2	IPv6 Internet	IPv6 Internet	3 - ICMP ICMPv6 E ICMPv6 E
Authorized to configure Firewall			
1	10.0.1.0/255.255.255.0	FW_CL_10.4.0.111-0	Aker - AS
Enables Aker Authentication & socks/www proxies			
1	10.0.0.0/255.255.255.0 10.0.0.11	FW_CL_10.4.0.111-0	Aker - CL HTTP HTTPS Socks 5

To accept rules press 'Finish' otherwise press 'Cancel' to quit and loose all changes.

Image 201 – *Filtering rules wizard* closing notice

7.6. Using the Pipes rules

This window was created in order to organize your Q.O.S rules. In Aker Firewall it is known as Pipe. It allows visualizing in only one window all of your PIPE rule, without the need of visualizing several windows as the General Filtering rules or Filtering rules in the access profile.

The fields are similar with the Filtering Rules window, containing:

- **Source:** Establishes the source network/IP packets
- **Destination:** Establishes the destination network/IP packets;

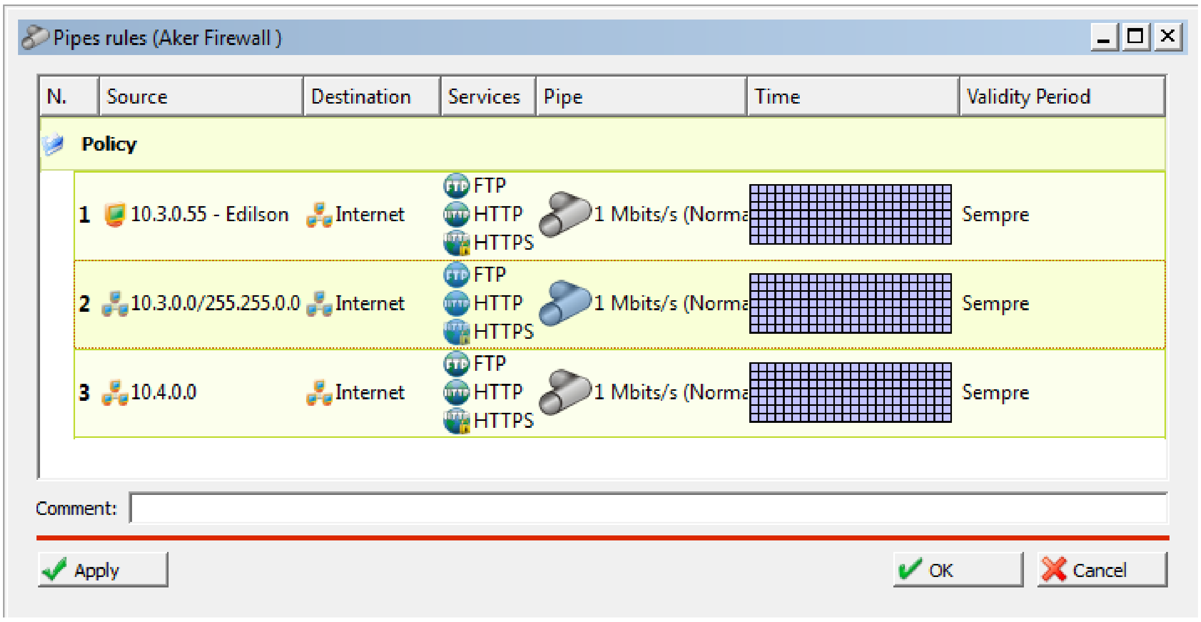
- **Services:** Allows to select which services (TCP, UDP, ICMP or other) will use this PIPE rule;
- **Pipe:** The administrator can set a different Quality of Service (QoS) for each type of rule;
- **Time:** Defines time and day of the week that the rule will be applicable. The lines represent the days of the week, and the columns represent the time. In case you wish to make the rule applicable in a specific time the check box must to be checked, otherwise the check box must to left in blank.

In order to facilitate your configuration, you can left click on the check box and drag it, keeping the button pressed. This way the tab will be modified as you move the mouse.

Validity Period: Allows registering two dates that delimit a period.

Comment: Add a comment about the rule. It is very useful in the documentation, and maintenance of information about the rule use.

Pipes rules window



N.	Source	Destination	Services	Pipe	Time	Validity Period
Policy						
1	10.3.0.55 - Edilson	Internet	FTP HTTP HTTPS	1 Mbits/s (Norma		Sempre
2	10.3.0.0/255.255.0.0	Internet	FTP HTTP HTTPS	1 Mbits/s (Norma		Sempre
3	10.4.0.0	Internet	FTP HTTP HTTPS	1 Mbits/s (Norma		Sempre

Comment:

Image 202 – Pipes rules window

Note: These rules override the configurations of “Pipe” from the General Filtering Rules and the Filtering in the access profiles.

Configuring the address translation

8. Configuring the address translation

This chapter will show how to configure the addresses translation parameters (NAT) in order to allow the Intranet work with the reserved addresses, increasing its addressing capacity, hiding the hosts in the Intranet and accessing the internet, in a transparent way. In this version you can also perform a connection load balancing in a smarter way.

8.1. Planning installation

What is addresses translation?

Any network that will connect to the Internet requires a set of addresses assigned by any authority designated for this purpose. Basically there are 3 sets of possible addresses, so-called: Class A (enables 16.777.214 hosts within the network), Class B (enables 65.533 hosts) and Class C (enables 254 hosts).

Due to the high growth presented by the Internet in the last years, there are no Class A and B addresses available. Thus, any network that connects will receive an address Class C which allows the addressing of only 254 hosts. In case the host number is larger than that, you have to purchase several Class C addresses which make difficult the administration work, or use an address translation.

Address translation is a technology that allows the host addresses from the Intranet be distributed freely, using Class A addresses. This way, it continues allowing all hosts having internet access in a simultaneously and transparently way to the internet.

Its functioning is simple, every time a host with a reserved address tries to access the Internet, the Firewall detects and automatically translates its address to a valid address. When the target host responds and sends data to the valid address, the Firewall translates back this address to the reserved one and passes the data to the internal host. The way it is done, neither clients hosts nor server hosts know about the existence of such mechanism.

Another advantage, beside the one presented above, is with an addresses translation all the hosts from your Intranet will be invisible to the external network, increasing even more the installation security level.

The address translation is not compatible with services that transmit IP addresses or ports as part of the protocol. The only services supported by Aker Firewall are FTP, Real Audio and Real Video.

Which are my Intranets?

The Intranets are made of all hosts of one or more subnets which are being protected by Aker Firewall. This includes all the internal devices from the network, as routers, switches, server hosts, client hosts, etc. They are the equipment that saves the important information from your network, or are key parts for its functioning.

Which are my external networks?

The external networks are made of all hosts that do not belong to the Intranet. They may or may not be under the administrative responsibility of your organization.

In case an organization network is connecting to the internet, the external network would be the entire Internet.

Addressing my Intranet

Although technically possible, the Intranet addresses should not be chosen randomly. There are few addresses reserved specifically for this purpose. These addresses cannot be assigned to any host connected to the Internet.

The reserved addresses are:

From **10.0.0.0** to **10.255.255.255**, mask 255.0.0.0 (class A)
From **172.16.0.0** to **172.31.0.0**, mask 255.255.0.0 (class B)
From **192.168.0.0** to **192.168.255.255**, mask 255.255.255.0 (class C)

Types of address translation

There are 3 different types of addresses translation: 1-1, N-1, 1-N e N-N. Each has distinct features and normally they are used in set to get better results.

- **1-1**

  The **1-1** is the more intuitive, but normally is the less useful. It consists of making binary mappings one-to-one among the reserved addresses and the valid addresses. This way, distinct hosts would have different converted addresses.

  The major limitation of this form of operation is that is not possible to put a number of host larger than the number of valid addresses, once they are always converted on a one-to-one basis.

- **N-1**

The ***N-1*** allows many hosts with reserved addresses use a same valid address. To achieve this goal, it uses IP addresses in combination with ports (for TCP and UDP protocols) or with sequence number (for ICMP). This mapping is done dynamically by the firewall, every time a new connection is established. As there are 65535 ports or different sequence numbers, it is possible the existence of 65535 simultaneous active connections using the same address.

The only limitation of this technology is that it does not allow internal hosts to be accessed externally. All the connections must to be initiated internally.

When using the address translation (NAT) ***"N: 1"*** on Aker Firewall, beside the IP addresses translation from the Intranet to a single valid IP to the internet, the source port of communication is also changed.

All communication based in TCP/IP protocol, have at least the following parameters:

- Source IP;
- Source port;
- Destination IP;
- Destination port.

Example: The computer IP address is 200.0.0.1 and the IP address from the web site *EBay* (http://www.ebay.com) and 66.211.181.181, so the connection is:

- Source IP: 200.0.0.1
- Source port: Any port between 1024 and 65535
- Destination IP: 66.211.181.181
- Destination port: TCP 80 (HTTP)

From Aker Firewall 6.1 Patch 3 or higher, this source port value when using the "N: 1" address translation varies between the values 8176 up to 63487. The port range can be changed, as the example below:

Solution:

Edit the file ***"rc.aker"*** at the location ***/aker/bin/firewall***. Change the line:

Insmod $MODNAME

To: insmod $MODNAME nat_init=20000 nat_end=40000

Where:

- nat_init= <source port beginning >

- nat_end= <source port max. value>

The default values are:

- nat_init= 30720
- nat_end=63472

- **1-N**

  This type of address translation is also called of load balancing and allows several servers to be placed behind a single valid IP address. Every time a new connection is opened to this address, it is redirected to one of the internal servers. A great advantage of this technology is the enabling of services that require a large amount of resources, can be separated in several hosts and be accessed in a transparently way, through a single address. In case some of these hosts crash, the new connections are automatically passed to the hosts which remain online, implanting a mechanism of fault tolerance.

- **N-N**

  This address translation allows all the addresses of a network to be translated to the addresses in a virtual network automatically.

Address translation applications with Aker Firewall

Aker Firewall allows any type of address translation to be performed, not limited only to the valid address of the firewall external interface, but giving total flexibility to the administrator to use any address within the network, including making the address translation between invalid networks.

Suppose a particular organization receives a class C address, format A.B.C.0. This is a valid address that supports a maximum of 254 hosts (the addresses A.B.C.0 and A.B.C.255 are reserved for a specific purpose and cannot be used, remaining the values from A.B.C.1 to A.B.C.254) assuming that this network has 1000 hosts to be connected. Due to the inability to allocate all hosts in the received address, it has been decided the use of address translation. A *“Class A”* reserved address has been selected to be placed in the Intranet hosts, 10.x.x.x mask 255.0.0.0.

Aker Firewall will be placed between the Internet and Intranet which has reserved addresses. Aker Firewall will be responsible for the translation of reserved addresses 10.x.x.x to the valid addresses A.B.C.x. This way the Firewall shall have at least two addresses: a valid address which can be reached by the Internet, and a reserved address which can be reached by the Intranet. (most installations, place two or more network adapters in the firewall: one for the external network and the other for the Intranet. Although is possible, but no recommended to make the same setting only with one network adapter, assigning a valid and a reserved address to the same network adapter)

Suppose an A.B.C.2 address has been chosen for the valid section and 10.0.0.2 for the reserved section. The valid address will be used by the firewall to translate all the connections originated in the Intranet and destination on Internet. Externally all the connections will be seen as they came from this valid address.

Another example would be an organization which has Internet outputs and 3 classes of valid addresses, in this case the administrator is able to distribute the address translation among these three classes, gaining more flexibility in configuration.

With the address translation working, all internal hosts can access any internet resource transparently, as they have valid addresses. However it is not possible to any external host initiate a connection to any internal host (because they do not have valid addresses). To solve this problem, Aker Firewall enables the *translation rule configuration 1-1*, which allows simulating valid addresses to any reserved address.

Going back to our hypothetical organization, suppose in your network there is a WWW (WORLD WIDE WEB) server, address 10.1.1.5 and you want this serve to provide information to the Intranet and to the Internet. In this case a valid address must to be chosen in order to the external clients use this address to connect to this server. Suppose the chosen address is A.B.C.10, an address translation rule 1-1 must to be added, in order to map the address A.B.C.10 to the internal address 10.1.1.5. From this moment, all the accesses to A.B.C.10 will be automatically mapped again through the firewall to 10.1.1.5.

The valid addresses chosen to perform the address translation 1-1 cannot be assigned to any real host. This way, in our example is possible the configuration of up to 253 servers in your Intranet that can be accessed externally (one of the 254 valid addresses is already used to translate the traffic of all client hosts.

Aker Firewall uses the technology ***proxy-arp*** to enable the virtual servers to be treated by the hosts within the valid network (e.g. the external router) as they were real hosts.

Examples of configurations using address translation:

- **Connecting to the Internet with a dedicated line**

Equipment: 1 router, 1 *Aker* Firewall, n clients, 2 servers in the Intranet
Valid address: A.B.C.x, network mask 255.255.255.0
Reserved address: 10.x.x.x network mask 255.0.0.0
Serves address: 10.1.1.1, 10.2.1.1
Clients address: 10.x.x.x
Router address: Valid network A.B.C.1, Internet :x.x.x.x

Aker Firewall configuration:

Network adapters addresses: Intranet: 10.0.0.2, Valid network A.B.C.2
Virtual IP for address translation N-1: A.B.C.2
Private network: 10.0.0.0
Private network mask: 255.0.0.0

Address Translation rules 1-1:

A.B.C.10 – 10.1.1.1
A.B.C.30 – 10.2.1.1

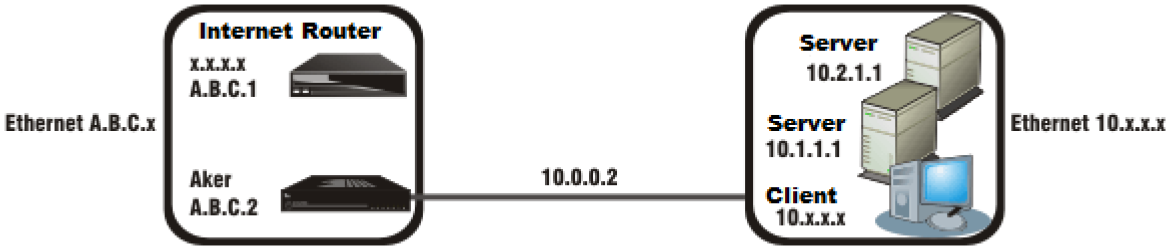

Internet Router
x.x.x.x
A.B.C.1
Ethernet A.B.C.x
Aker
A.B.C.2
10.0.0.2
Server
10.2.1.1
Server
10.1.1.1
Client
10.x.x.x
Ethernet 10.x.x.x

Image 203 – 1st example of Aker Firewall configuration (*linking departments*)

- **Linking departments**

This example shows how to link departments of the same company, using the address translation between these departments.

Equipment: 1 router, 3 *Aker* Firewall, any clients, 4 servers in the Intranet
Valid address: A.B.C.x, network mask 255.255.255.0
Reserved address: 10.x.x.x network mask 255.255.0.0
Reserved address:172.16.x.x, mask 255.255.0.0

Sub network address 1:

10.1.x.x
Server address: 10.1.1.1
Client address: 10.1.x.x
Router address: Valid network A.B.C.1 , Internet: x.x.x.x

Aker Firewall configuration:

Intranet: 10.1.0.1, Valid network A.B.C.2
Virtual IP for address translation N-1: A.B.C.2
Private network: 10.0.0.0
Private network mask: 255.0.0.0

Sub network address 2:

Externally: 10.1.0.2
Internally:172.16.x.x

Server address: 172.16.1.1
Client address: 172.16.x.x

Aker Firewall configuration:

Sub network 2: 172.16.0.1, Sub network 1:10.1.0.2
Virtual IP for address translation N-1:10.1.0.2
Private network (2): 172.16.0.0
Private network mask: 255.255.0.0

Address translation rules 1-1:

10.2.1.1 – 172.16.1.1

Sub network address 3:

Externally: 10.1.0.3
Internally:172.16.x.x

Server address: 172.16.1.1
Client address: 172.16.x.x

Aker Firewall configuration:

Sub network 3: 172.16.0.1, Sub network 1:10.1.0.3
Virtual IP for address translation N-1:10.1.0.3
Private network (3): 172.16.0.0
Private network mask: 255.255.0.0

Address Translation rules 1-1:

10.3.1.1 – 172.16.1.1

In the routing table for this type of installation we should insert routes to the network 10.1.x.x, 10.2.x.x, 10.3.x.x

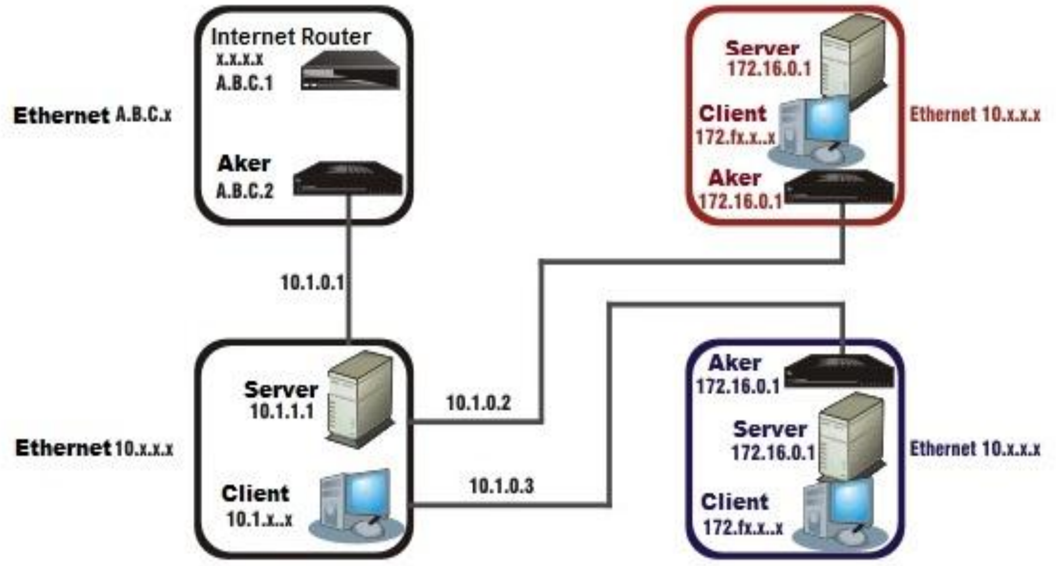

Internet Router
x.x.x.x
A.B.C.1
Ethernet A.B.C.x
Aker
A.B.C.2
10.1.0.1
Server
172.16.0.1
Client
172.fx.x..x
Aker
172.16.0.1
Ethernet 10.x.x.x
Server
10.1.1.1
Client
10.1.x..x
Ethernet 10.x.x.x
10.1.0.2
10.1.0.3
Aker
172.16.0.1
Server
172.16.0.1
Client
172.fx.x..x
Ethernet 10.x.x.x

Image 204 – Example 2 of Aker Firewall configuration (*multiple connections with the internet*)

- **Multiple connections with the Internet**

In this example much more complex, we will show how to use 3 connections with the Internet and two Intranets, using the address translator between them.

Equipment: 3 routers, 1 *Aker* Firewall, any clients, 2 servers in the DMZ network
Valid addresses: A.B.C.x, D.E.F.x, G.H.I.x, all with network mask 255.255.255.0
Address reserved for the Intranet: 10.x.x.x network mask 255.0.0.0
Address reserved for the DMZ:172.16.x.x, mask 255.255.0.0
Routers addresses: Valid network A.B.C.1, D.E.F.1, G.H.I.1 , Internet :x.x.x.x

Aker Firewall configuration:

Network adapters addresses: Adapter 1: 10.0.0.2, Adapter 2: 172.16.0.2 , Adapter 3: A.B.C.2, Adapter 4: D.E.F.2, Adapter 5: G.H.I.2
Private network: 10.0.0.0 e 172.16.0.0
Private network mask: 255.255.0.0

DMZ servers
Web server – 10.0.0.10
SMTP server – 10.0.0.25

Address translation rules

1. Source – 10.0.0.10 translate to A.B.C.10 when it is used for the Internet
2. Source – 10.0.0.25 translate to D.E.F.25 when it is used for the Internet
3. Source – 172.16.x.x translate to 10.0.0.4 when it is used for the network 10.0.0.0
4. Source – 172.16.x.x translate to D.E.F.25 when it is used for the Internet
5. Source – 10.x.x.x translate to A.B.C.20 when it is used for the Internet

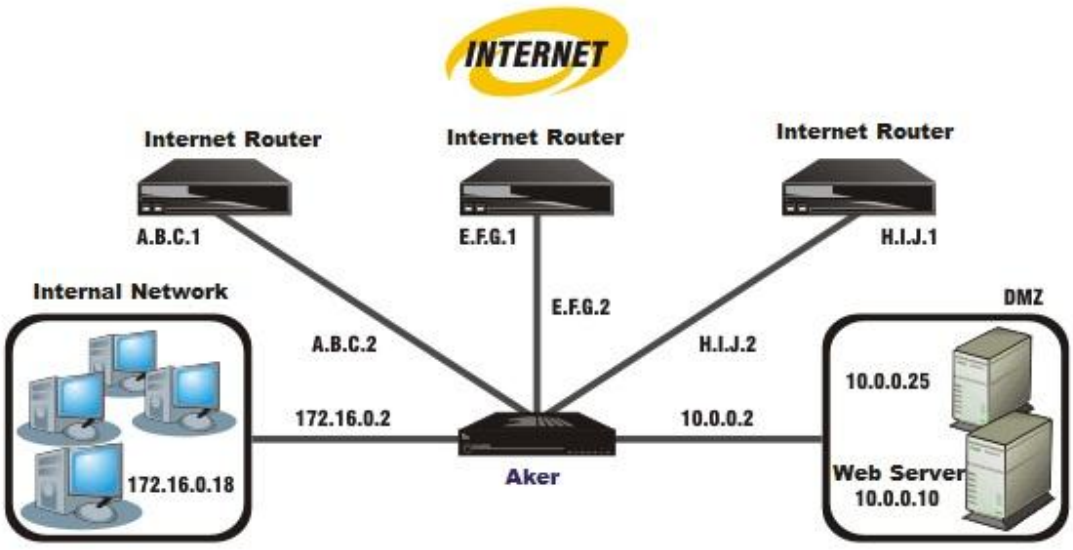


Image 205 – 3rd Example of Aker Firewall configuration (*setting up the address translation rules*)

With Aker Firewall is possible to do a link balancing in order to perform a more optimal use of links. The Firewall has verification mechanisms of the activation of links, being possible to split the traffic in a smart way through links or divert the traffic from the one which is offline.

The administrator can also assign weights to his connections, so the faster connections may also have a greater weight than the slower connections, this way the firewall will give preference to send the traffic to the link with greater weight.

Setting up the address translation rules for Aker Firewall

Configure address translation rules in Aker Firewall is something easy because of its intelligent design. All part of IP addresses, masks, protocols and ports are configured in the entities (for more information, see the chapter titled ***Registering Entities***). Due to it, when configuring a rule, it is not necessary to worry about which port a specific service uses or what is a network or host IP address. All of it has already been registered. To make it even easier, all the services most used on the Internet are already pre-configured from factory, being unnecessary to waste time searching the data for each one of them.

Basically to register an address translation rule, you have to specify the source and destination entities, virtual interface and service (if it is the case).

The address translation functioning is simple: the firewall will search one by one the rules defined by the administrator, in the specific order, until the packet fits in one of them. From this moment, the firewall will execute the address translation type associated to the rule. In case the search reaches its end and the packet does not fit in any rule then it shall be translated.

Using the Remote Interface

To gain access to the address translation configuration window, follow the steps below:

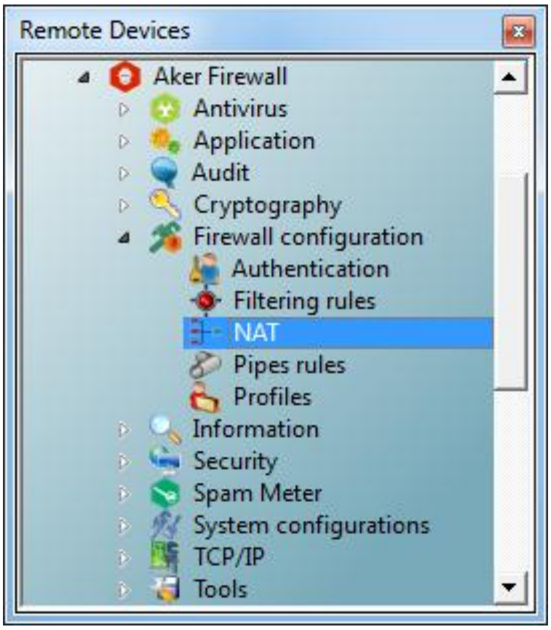
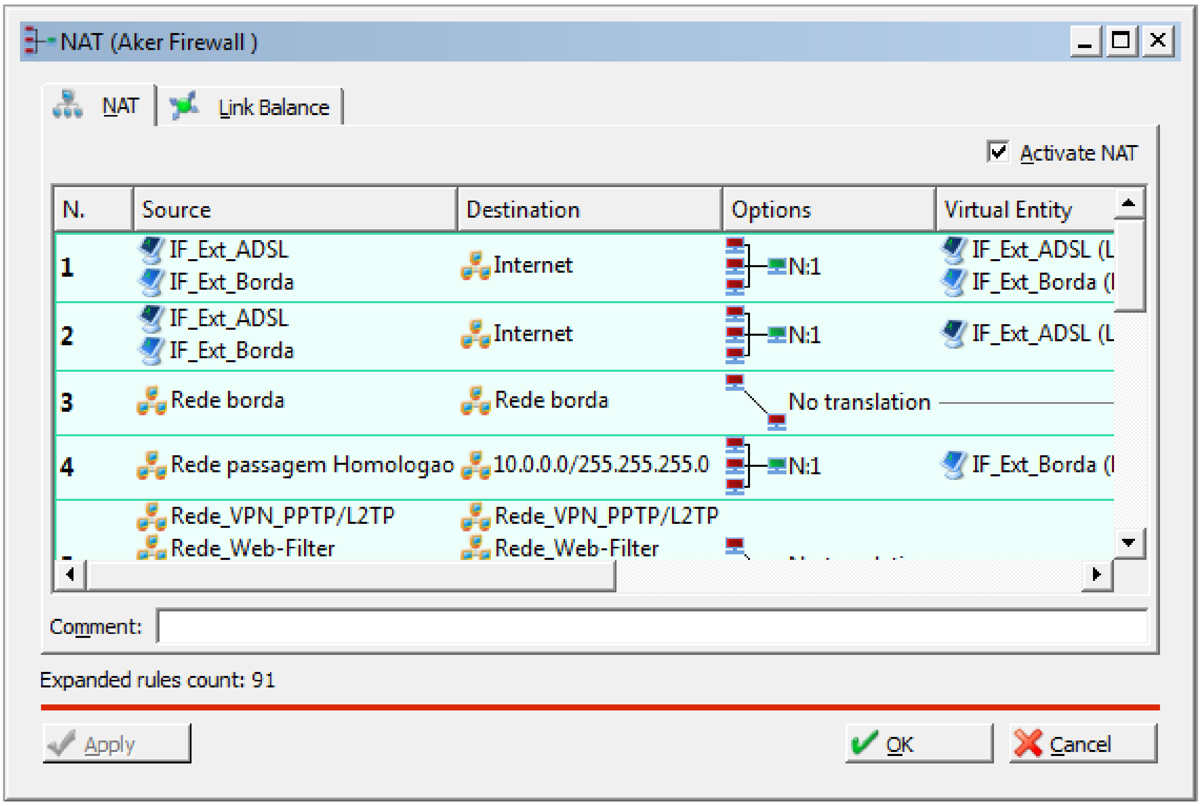

Remote Devices
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Authentication
Filtering rules
NAT
Pipes rules
Profiles
Information
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 206 – *Address translation* configuration window.

- Click on the *Firewall configuration* menu.
- Select *NAT*.

***Address Translation* configuration window (NAT)**



☑ Activate NAT

N.	Source	Destination	Options	Virtual Entity
1	IF_Ext_ADSL IF_Ext_Borda	Internet	N:1	IF_Ext_ADSL (L IF_Ext_Borda (I
2	IF_Ext_ADSL IF_Ext_Borda	Internet	N:1	IF_Ext_ADSL (L
3	Rede borda	Rede borda	No translation	
4	Rede passagem Homologao	10.0.0.0/255.255.255.0	N:1	IF_Ext_Borda (I
	Rede_VPN_PPTP/L2TP Rede_Web-Filter	Rede_VPN_PPTP/L2TP Rede_Web-Filter		

Comment:

Expanded rules count: 91

Image 207 – *Address Translation* configuration window (NAT).

The address translation window contains all the translation rules defined in Aker Firewall. Each rule will be displayed in a specific line, consisting of several cells. If a rule is selected, it will be displayed in a different color.

- The **OK** button will update the rule set and run immediately.
- The **Apply** button will send to the firewall all the made changes, but it will keep the window opened.
- The **Cancel** button will discard all the made changes and close the window.
- There is a bar to add comments on the address translation rule.

- IF the **Activate NAT** option is checked, the firewall will translate the addresses according to the registered rules. In case it is not checked, no translation will be made.

- The scroll bar on the right side is used to show the rules that do not fit in the window.
- When clicking on a rule and selecting it, if it has a comment this comment will be displayed at the bottom of the window.
- The rule position can be changed by clicking and dragging the mouse to the new position.

The window contains the following fields:

Source: This field specifies a list of all entities whose addresses will be translated to the Virtual Entity address described above. The address translation 1-1 or address translation services allow only one entity be selected for this field and this entity must be of host type.

In case the 1-N translation or Services Translation 1-N are being used, each host belonging to this field will have a weight assigned to it, showing between parentheses, on the right of the entity name. To change the weight of a specific host, i.e., making it receive more connections, the other must to right-click on the entity name, in the list on the right, select the option *Change weight* and choose a new value.

The Source Entity field must to contain the internal addresses (reserved or non-valid) from the participating hosts of the address translation, regardless of its type.

Destination: This field is used to specify the entities whose address translation will be performed (in case of address translation N-1) or the host which will access the internal hosts through the address contained in the Virtual Entity field (for the other types of translation). When creating several rules with different values in this field, cause the same host has its addresses translated into different addresses depending on the communication destination.

The most common value for this field is the specification of the *Internet* entity with the destination.

Options: Type of NAT that shall be used.

Virtual Entity: In this field you must to configure the entity which the internal addresses will be translated for or which the external requests must to be directed to.

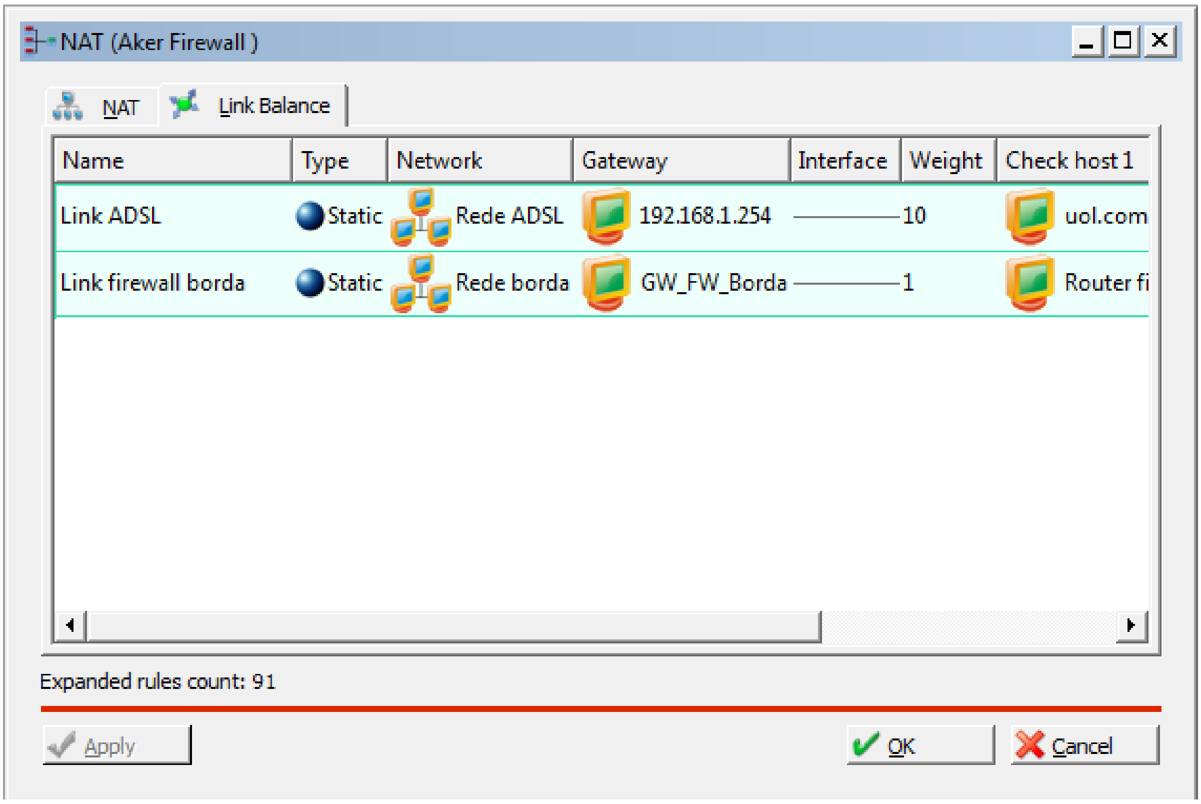
Services: This field defines which services will be part of the rule, when using the translation of services, N-1 services or translation1-N with services. The window will be unable for other types of translation.

Virtual Services: Service which will be translated, only used in *NAT port.*

Link balancing: This field allows enabling or disabling the link balancing. The configurations must have been performed when this option is selected.

Comment: Reserved to add a description about the rule. It is very useful in the documentation, and maintenance of information about its use.

Link Balance configuration window



Name	Type	Network	Gateway	Interface	Weight	Check host 1
Link ADSL	Static	Rede ADSL	192.168.1.254		10	uol.com
Link firewall borda	Static	Rede borda	GW_FW_Borda		1	Router fi

Expanded rules count: 91

Image 208 – *Link Balance* configuration window.

- The **OK** button updates the set of rules, and activates it immediately.
- The **Apply** button sends to the firewall all the made changes, but the window will remain opened.
- The **Cancel** button discards all the made changes and closes the window.

This tab contains the following fields:

Name: In this field a name must to be informed to represent the Internet provider;

Type: This field informs the configuration type: Static or Dynamic.

Selecting the *static* link, it is mandatory to register a network entity and a host entity (gateway), in this case it is not allowed to register a network interface entity. When the link is *dynamic*, the situation is reversed, and the user is forced to register an entity *interface type* (the registration of entities network, and host (gateway) are not allowed).

Network: Register the network which the Internet provider has provided;

Gateway: The Internet Provider router IP must to be informed (in this case the firewall will perform a review in order to verify if the gateway belongs to the Provider's network);

Interface: This field is used for the registering of entity network interface type, which will represent the dynamic link.

Weight: Indicates a value which the link will be assigned. When the weights are larger assumes that the links are faster.

Check Host 1: In this filed must be registered an entity which follows the Internet Provider's router. This entity will be used by the firewall to specify whether the link is online or not. A DNS server from the *Internet Provider* or even from near routers can be registered.

Check Host 2 e Check Host 3: Checks entities also used by the firewall. It is not mandatory the registration of the three Check entities, however, as much entities registered better will be to the firewall check system.

To perform any operation on a specify rule, simply right-click on it. The following menu will be displayed (this menu will be activated every time the right button is pressed, even when there are no selected. In this case, only the options *Insert* and *Paste* will be enabled).

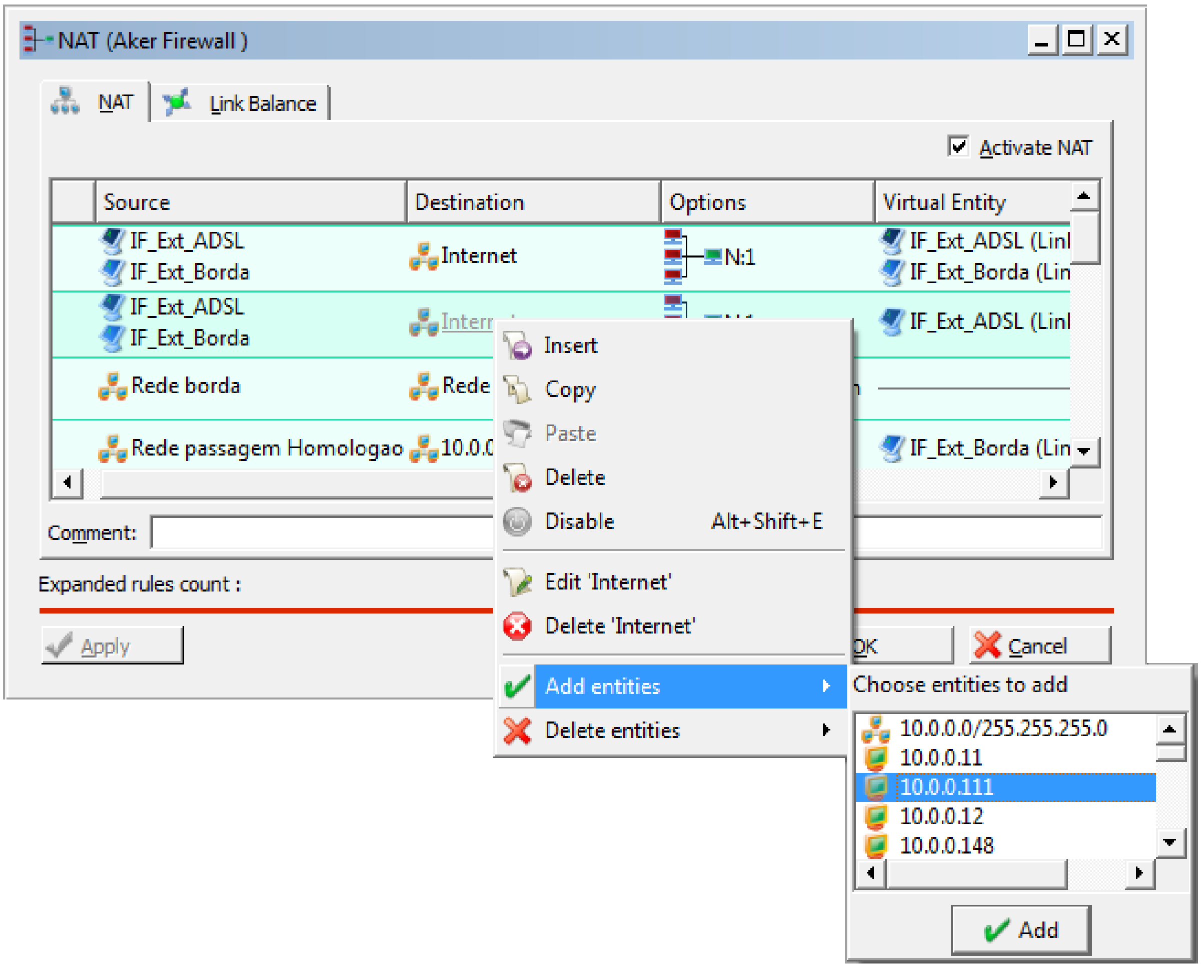

NAT (Aker Firewall)
NAT
Link Balance
☑ Activate NAT
Source
Destination
Options
Virtual Entity
IF_Ext_ADSL
IF_Ext_Borda
Internet
N:1
IF_Ext_ADSL (Linl
IF_Ext_Borda (Lin
IF_Ext_ADSL
IF_Ext_Borda
Interr
IF_Ext_ADSL (Linl
Rede borda
Rede
Rede passagem Homologao
10.0.0
IF_Ext_Borda (Lin
Comment:
Expanded rules count :
Apply
OK
Cancel
Insert
Copy
Paste
Delete
Disable Alt+Shift+E
Edit 'Internet'
Delete 'Internet'
Add entities
Delete entities
Choose entities to add
10.0.0.0/255.255.255.0
10.0.0.11
10.0.0.111
10.0.0.12
10.0.0.148
Add

Image 209 – Adding entities configuration window

- **Insert:** Allows the inclusion of a new rule in the list. If any rule is selected, the new rule will be added replacing the old rule. Otherwise the new rule will be added at the end of the list.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes the copied rule to the list. If a rule is selected, this rule will be replaced for the new one, otherwise the new rule will be added at the end of the list.
- **Delete**: Removes the selected list from the list.
- **Enable/Disable:** This option allows enabling or disabling the selected rule, i.e., it will remain registered, but the firewall will behave as this rule does not exist (in case of *Disable*) and will continue the search on the next rule.
- **Add entities:** Adds a new entity.

Hint: The easiest way for an administrator assembles his translation rule will be dragging the entity and dropping them into the rule.

Hint 2: The position of each rule can be changed, simply clicking and dragging the rule to the new position.

In case of adding or editing rules, the window below will be displayed:

Adding NAT rules window

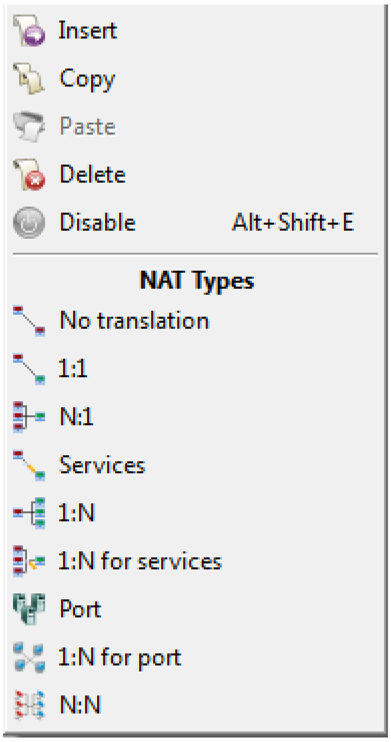


Image 210 – Adding NAT rules windows.

NAT types: This field defines the type of address translation which will be performed.

It has the following options:

- **No translation:** This option indicates to the firewall, that it must not have address translation when any hosts belonging to the Source Entities attempt to access any hosts belonging to the Destination Entities and vice versa.

- **Translation 1-1:** This option indicates to firewall when the host listed in the Source Entities attempt to access any host belonging to the *Destination Entities*, this specific host will have its address translated to the address of the *Virtual Entity*. Every time a host belonging to the *Destination Entities* access the *Virtual Entity* address, this access will be the last one translated automatically for the real address, defined by the entity exiting in the Source Entities. This type of translation is useful to enable the external access to internal servers.

For the Source Entities, must be placed an entity with the real address (internal or reserved) of the host which the translation 1-1 will be performed. For the *Virtual Entity* must to place an entity with the address which the internal address will be converted to (valid address), and will be accessed by the external hosts.

- **Translation N-1**: This option indicates to the firewall when any host listed in the Source Entities attempt to access any hosts belonging to the *Destination Entities*, this specific host will have its address translated to the address of the *Virtual Entity*. This type of translation is useful to enable a large number of hosts use only one valid IP to communicate through the internet, however it does not allow the external hosts (listed in the *Destination Entity*) start any communication with the internal hosts (listed in the *Source Entities*)

When the Cluster module is working on the translation N-1, the Virtual Entity IP cannot be assigned to the firewall interfaces.

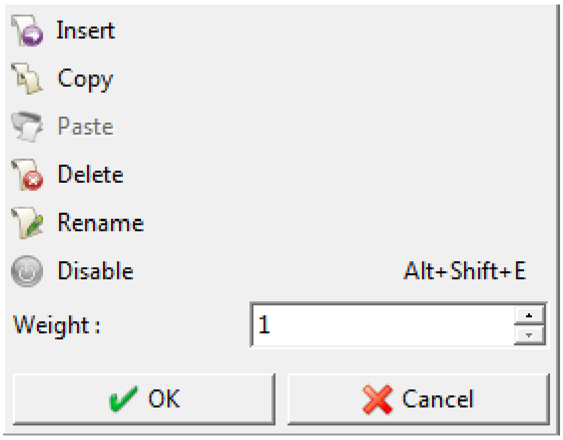
- **Services translation**: This option is useful for networks which have only one IP address and need to enable the service to the Internet. It enables that specifics services, being accessed in the firewall, be redirected to the internal hosts.

In the Source Entities field, must to place the internal IP address of the host which the services will be redirected. In the Destination Entity field, must be placed the hosts that will access the services externally. In the Service field must to choose all the services that will be redirected to the existing host in the Source Entities when the existing host in the Destination Entities access them in the Virtual Entity IP address.

When the Cooperative Cluster module is working the service translation is not possible.

- **Translation 1-N**: This option is used to perform the load balancing, i.e., enable several hosts to respond as one.

In the *Source Entities* field must be placed the hosts which will be part of the load balancing and will begin to respond as one. In the *Destination Entities* field, must be placed the hosts which will access the internal hosts specifying the existing entity in the *Virtual Entity*.



Weight : 1

Image 211 – *Weight* configuration window.

- **Translation 1:N for services:** This option is used to perform the load balancing for specific services, i.e. , allowing several hosts respond the requests from this service as they were one.
- **Port**: This type of NAT is used to perform translations of IP addresses, and ports for connections, and it is also known as PAT (port address translation).
- **1:N for port**: Does the server balancing performing translations of IP address and connection ports, and after the translation, the accesses are distributed among the servers which are part of the balancing.

- **Translation N:N**: This option indicates to the firewall that the addresses belonging to the network listed in the Source Entities, when accessing any hosts belonging to the Destination Entities, it will be converted to the network addresses in the Virtual Entity field, i.e. , for this translation must be used a network entity in the source column and a network entity in the virtual entity column. The destination field can be filled in the same way as the other types of NAT.

In addition, the source entity and virtual entity network masks need to be equal so the NAT works.

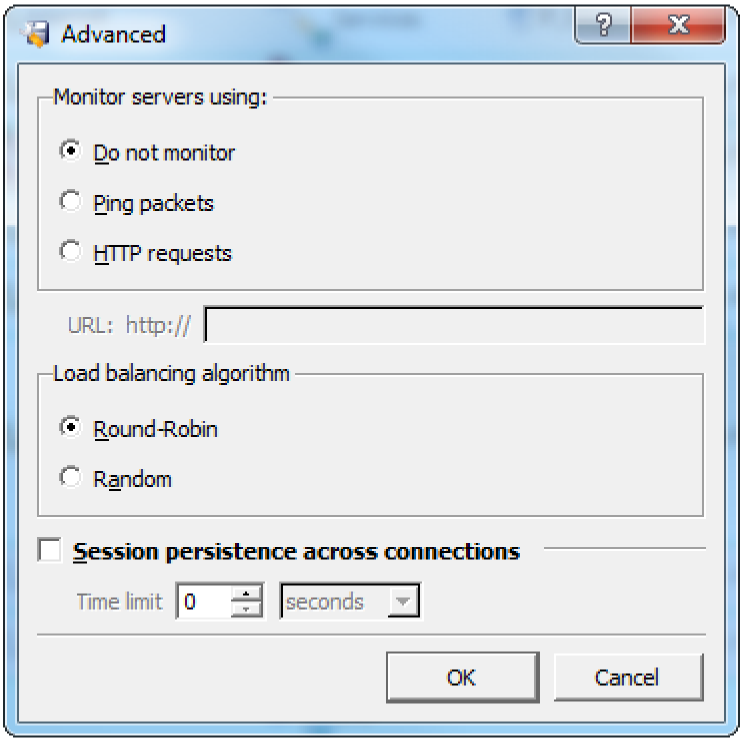
E.G.

	IP	Network Mask
Source	192.168.0.0	255.255.255.0
Virtual Entity	172.16.0.0	255.255.255.0

Image 212 – Source entity and virtual entity network masks need to be equal.

- In the example above, all networks IPs 192 will be translated to the 172.

The **Advanced** option is enable only when the address translation 1-N or Service translation is selected, this option allows configuring the parameters of configuration which will be performed by the firewall in order to detect if the balancing participating hosts are online or not, and how the balancing will be performed. When selecting this option the following window will be displayed:



Monitor servers using:

● Do not monitor

○ Ping packets

○ HTTP requests

URL: http://

Load balancing algorithm

● Round-Robin

○ Random

☐ Session persistence across connections

Time limit 0 seconds

Image 213 –Monitoring to be performed by the firewall.

Types of monitoring

The **Monitor servers using,** allows the definition of the method used by the firewall to verify if the balancing participating hosts (hosts defined in the *Source Entities* field) are online. It consists of the following options:

Do not monitor: Selecting this option, the firewall will not monitor the hosts and assume that the hosts are active.

Ping packets: Selecting this option, the firewall will monitor the hosts through the ICMP packets of *Echo Request* and *Echo Reply* (that are also used by the PING command).

HTTP requests: Selecting this option, the firewall will monitor the hosts through the HTTP requests. For this option, the URL which the firewall will attempt to access each host in order to verify if it is active or not, the URL must be specified (without the prefix http://)

Load balancing algorithm: This field allows the definition of the method used to balance the requests among the hosts existing in the *Source Entities* field. It consists of the following options:

Round-Robin: Selecting this option, the firewall will distribute sequentially the requests to the participating hosts of the balancing, one-by-one. In case the hosts have different weights, first a connection will be distributed to each host, and then a connection will be distributed to each host which has received a number of connections smaller than its weight and so on. When all the connections receive a number of connections equivalent to its weight, the algorithm is started.

Random: Selecting this option, the firewall will distribute the connections in random way among the hosts, i.e., the probability of a connection be redirected to a specific host is equal the ratio between its weight and the total weight of all hosts.

Session persistence across connections: This field allows the definition of the session persistence across connections time or applications that use more than one connection in different times, i.e., the maximum waiting time for a new connection after the first connection ends.

Notes about the rules mounting.

It is highly recommend that the translation rules be placed in the following order:

1. *No address translation* rules;
2. *Services address translation* rules;
3. *Address translation 1-1 and N-N* rules;
4. *Services address translation 1-N* rules;
5. *Address translation 1-N* rules;
6. *Address translation N-1* rules;
7. *Address translation N-N* rules.

It is necessary the inclusion of a *No Transtion* rule originated in the Intranets and with destination in the Intranet as well, if you intend to administrate the firewall through a internal host which will participate of any type of translation. This rule shall be placed before any other translation rules.

Example 01- Address Translation

Let us suppose a company has hosts and services described below, and wish to implement NAT. The company has a dedicated Internet connection, and its provider has distributed a valid IP addresses range on the Internet from 200.120.210.0 to 200.120.210.63.

In rule #1, we select the *No Translation* option for the company's Intranets (DMZ and Internal). This rule is important, because if any Intranet host manage the firewall, it will not have its address translated, which enables administration. It would also be correct to select *No Translation* option for administrator hosts (Source Entity), as well as for the interface through which the firewall will be managed (Destination Entity).

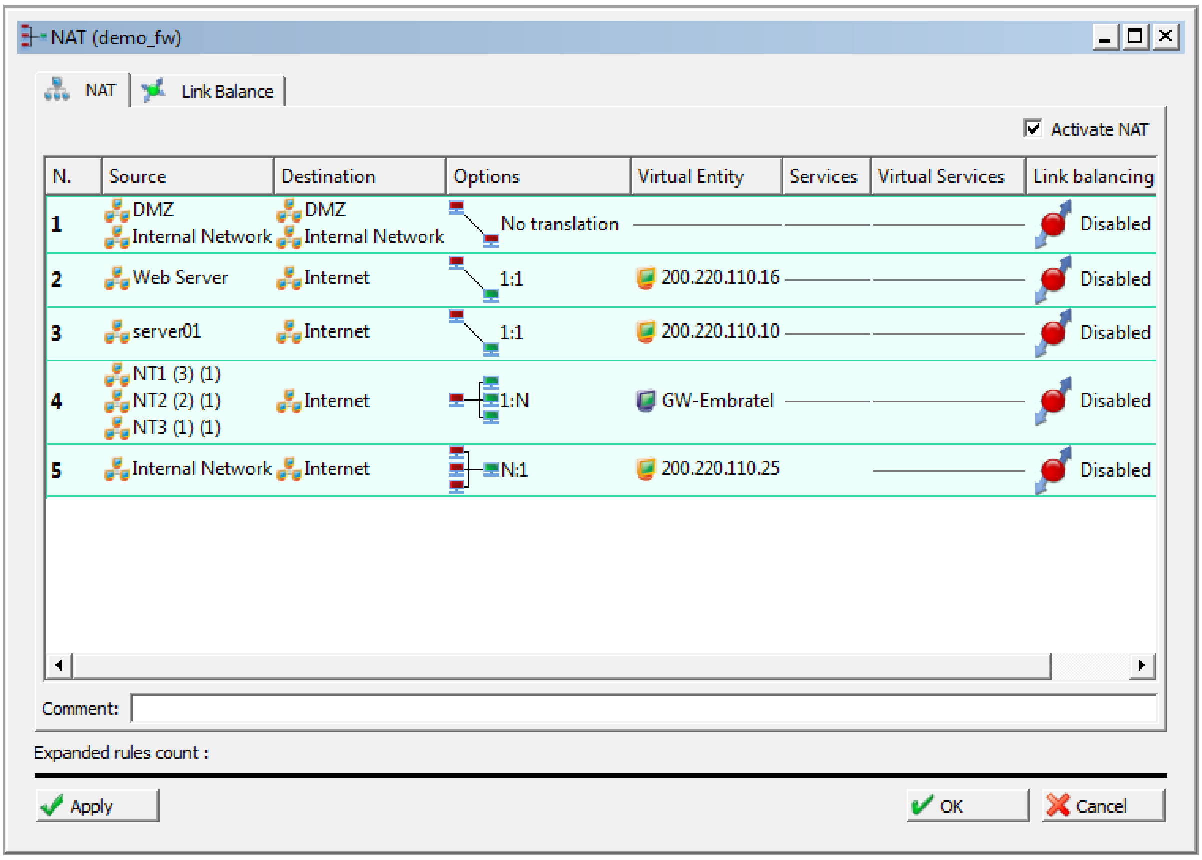
In rule #2, the *web server* will make a 1-1 translation to the address 200.120.210.15, which means that anyone on the Internet looking for IP 200.120.210.15 will be directed to *web server* (IP 10.20.0.50). The same way, if *web server* originates a connection to the Internet, its IP will be 200.120.210.15.

Rule #3 is identical to rule #2; the *server 01* will make a 1-1 translation to the 200.120.210.25 address.

Rule #4 exemplifies load balancing. Someone on the Internet looking for host 200.120.210.20 will be directed to NT3, NT2 or NT1, depending on the calculation made by the firewall. In the following case, the weights are different, therefore, host NT3, which has weight 4, will receive more connections. If the NT hosts have to originate Internet connections, they will have their addresses translated into 200.120.210.20 as well.

Rule #5 is of the N-1 translation type. Any Internal_Network host (10.20.0.0 with mask 255.255.255.0) will have its address translated into 200.120.210.16, when originating Internet connection. If someone from the Internet is attempting to connect with IP 200.120.210.16, the firewall will not direct it to any host in the Intranet, instead, it will discard packets to this connection, for not knowing which host the request should be sent to.

It is imperative to emphasize that the order of the rules in the list is of extreme importance. Let us suppose that **rule #2** is moved to the **last position**. In this case, someone looking for host **200.120.210.15** would be directed to *Web Server*. However, when originating an Internet connection, *Web Server* would have its address translated into **200.120.210.16**, because the rule that was in position 5 would perform the translation first.



☑ Activate NAT

N.	Source	Destination	Options	Virtual Entity	Services	Virtual Services	Link balancing
1	DMZ Internal Network	DMZ Internal Network	No translation				Disabled
2	Web Server	Internet	1:1	200.220.110.16			Disabled
3	server01	Internet	1:1	200.220.110.10			Disabled
4	NT1 (3) (1) NT2 (2) (1) NT3 (1) (1)	Internet	1:N	GW-Embratel			Disabled
5	Internal Network	Internet	N:1	200.220.110.25			Disabled

Comment:

Expanded rules count :

Image 214 – Example 01 (Address Translation)

Examples – Scenario 3 – Link Balancing

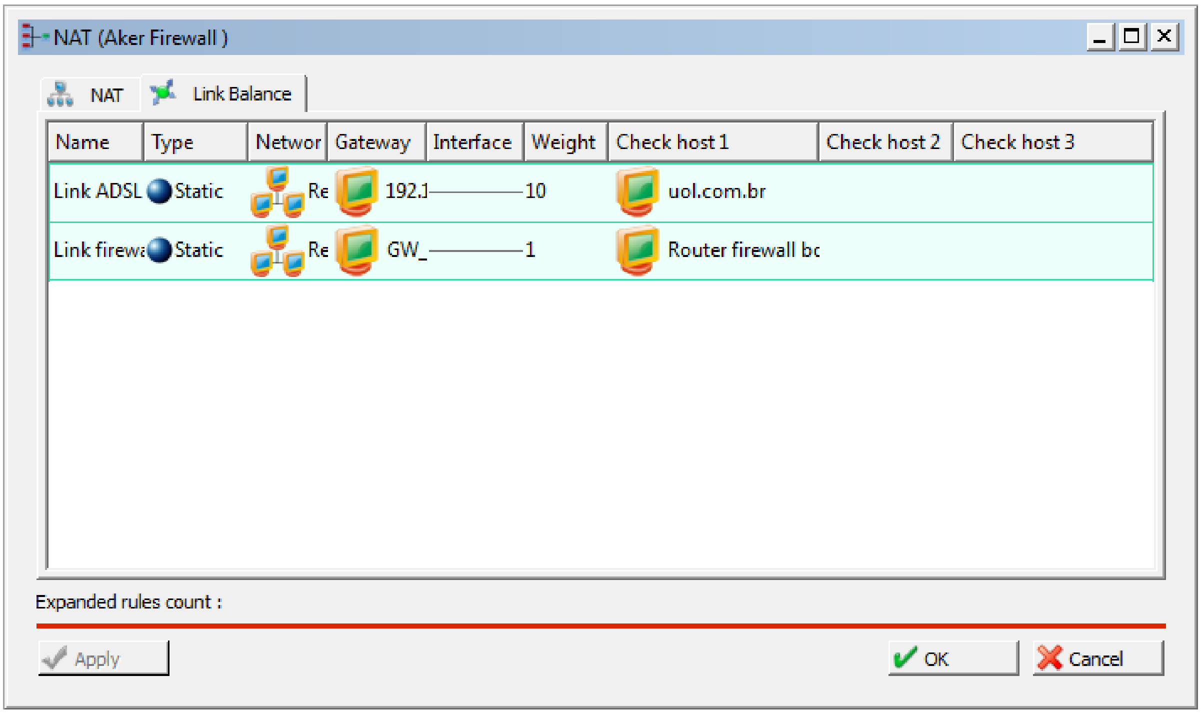
In this scenario will be described how to perform the links balancing. Suppose a company has two IP connection providers for Internet. In case the provider has provided its IP address range to the company.

Phase 1 – Mounting the balancing

The firewall administrator will perform the registration and inform the following entities and fields:

- **Name:** Informs the name to represent the provider link;
- **Type:** This field informs what type of configuration which can be "*Static*" or "*Dynamic*"
- **Network:** Registers the network given by the provider;
- **Gateway:** The provider router IP must be informed (in this case the firewall will make a critique in order to verify if the firewall really belongs to the provider's network) ;
- **Interface**: This field is used for the registration of entities network interface types, which will represent the dynamic link;
- **Weight:** Value which will be assigned to the link. When weights are larger assumes that the links will be faster.

- **Check host1:** Registers an entity that is right after the provider's router, preferably within one or two hops of your router. This entity is used by the firewall to specify if the link is online or not. A provider DNS server can be registered or even routers next to each other.
- **Check host 2 and Check host 3:** These are entities of verification also used by the firewall. It is not mandatory that the three entities of verification be registered; however as much entity registered you have better will be the firewall system verification.



Name	Type	Networ	Gateway	Interface	Weight	Check host 1	Check host 2	Check host 3
Link ADSL	Static	Re	192.1		10	uol.com.br		
Link firew	Static	Re	GW_		1	Router firewall bc		

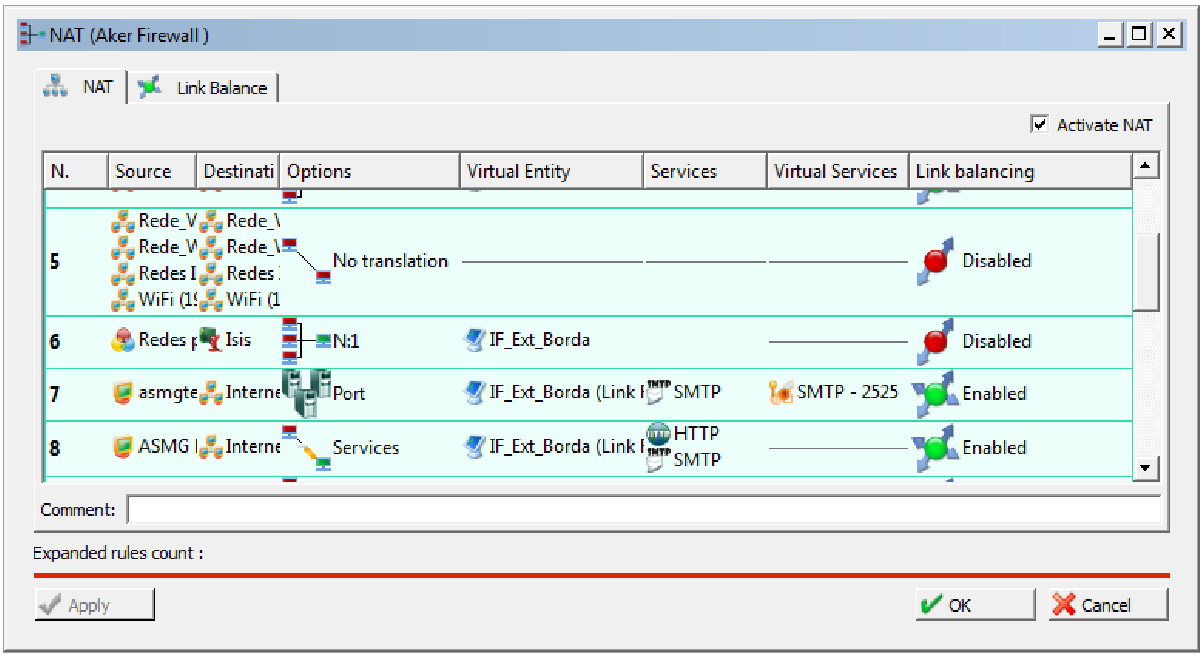
Image 216 – Link balancing (Phase 1).

Phase 2 – Mounting the NAT rules

The second phase is really simple, just place in each translation rule two or more Virtual entities

Do not forget to enable the corresponding icon in the Link balancing column so the service can be performed by the firewall. The firewall will perform a critique in order to determine if the *Virtual Entity* belong to a link previously registered.

There is a limitation when the connection is originated from the Internet. The DNS must to have duo IP entry and must run in Round-Robin mode. The problem is when a link of a specific provider goes off line the firewall does not divert the connection originated from the Internet. To work this problem out the administrator can use the scripts to remove from the DNS the provider's IP that is offline.


NAT (Aker Firewall)
NAT
Link Balance
☑ Activate NAT
Comment:
Expanded rules count :
Apply
OK
Cancel

N.	Source	Destinati	Options	Virtual Entity	Services	Virtual Services	Link balancing
5	Rede_V Rede_W Redes I WiFi (1!	Rede_\ Rede_\ Redes : WiFi (1	No translation	—	—	—	Disabled
6	Redes p	Isis	N:1	IF_Ext_Borda		—	Disabled
7	asmgte	Interne	Port	IF_Ext_Borda (Link I	SMTP	SMTP - 2525	Enabled
8	ASMG I	Interne	Services	IF_Ext_Borda (Link I	HTTP SMTP	—	Enabled

Image 217 – Mounting NAT rules (Phase 2)

8.2. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action)*, except it is not possible to configure the monitoring parameters.

Program location: /aker/bin/firewall/fwnat

Syntax:

```
Aker Firewall
fwnat – Configure the address translation rules (NAT)

Usage: fwnat [help | show | enable | disable]
fwnat [enable | disable | remove] <pos>
fwnat add <pos> 1-1 <source> <destination> [ <virtual entity> |
-bal <ev_1> <ev_2> ... ]
fwnat add<pos> n-1 <source> <destination> [ <virtual entity> |
-bal <ev_1> <ev_2> ... ]
fwnat add <pos> services <source> <destination> [ <virtual entity> |
-bal <ev_1> <ev_2> ... ] <service1>...<service2>
fwnat add <pos> ports <source> <destination> [ <virtual entity> |
-bal <ev_1> <ev_2> ... ] <service> <service virtual>
fwnat add<pos> No_translation <source> <destination>
fwnat add <pos> 1-n <source1>...<source2> <destination> [ <virtual entity> |
-bal <ev_1> <ev_2> ... ] <round-robin | random> <persist>
none | ping | HTTP <URL>>
fwnat add<pos> n-n <source> <destination> [ <virtual entity> | -bal <ev_1> <ev_2>
...]
```

Program help:

```
    deactivate    = disables address translation
    show      = shows all rules of the translation table
    add      = adds a new translation rule
    enable    = enables a translation rule
    disable  = disables a rule
    remove      = removes a translation rule
    help       = shows this message
```

To add:

```
    pos        = position where you add a new rule in the table
```

no_translation = do not perform translation between the source and destination

1-1 = perform servers translation. In this case, the source must to be mandatorily an entity host type

n-1 = performs the client translation

services = performs the translation only for the mentioned services.
In this case the source must to be mandatorily an entity host type.

ports = performs the translation only for the mentioned services.
In this case the source must to be mandatorily an entity host type. In addition, the service will be the<virtual service>

1-n = performs the load balancing, i.e., enables the access of several source hosts through the IP configured in the virtual entity, as they were a single host.
n-n = This translation allows all the addresses in a network be translated to the addresses of a virtual network automatically.

service1 = List of services names for the new rule, are accepted just for TCP or UDP protocol services

To enable / disable / remove:

pos = Number of the rule to be enabled, disabled or removed from the table.

For translation 1-n :

round-robin = Uses the round-robin algorithm for the balancing of connections
random = Uses the random algorithm for the balancing of connections
persist = Destination server persistence time (min) for connections originated from the same client
none = Does not monitor the source hosts, i.e. , consider they are always active

ping = Monitors the source hosts through pings
HTTP = Monitors the source hosts through HTTP connections
URL = Specifies which URL must to be used to monitor the hosts, in case the HTTP monitoring is being used

Example 1: (showing the configuration)

```
#/aker/bin/firewall/fwnat show
```

```
Global Parameters:
------------------

Address translation: Activated

Translation Rules:
-------------------

Rule 01
--------
Type: no_translation
Source: Intranet
Destination: Intranet


Rule 02
--------
Type: services
Source: Server
Destination: Internet
Virtual Entity: Firewall – external interface
Services: MYSQL      POP3        SMTP


Rule 03
--------
Type: 1-1
Source: Web Server_001
Destination: Internet
Virtual Entity: External Web server


Rule 04
--------
Type: n-n
Source: network1
Destination: Internet
Virtual entity: network2



Rule 05
--------
```

```
Type: 1-n
Source: server1,server2, server3
Destination: Internet
Virtual entity: Virtual Server
Balancing: random    Monitoring: http
URL: www.aker.com.br


Rule 06
--------
Type: n-1
Source: Intranet
Destination: Internet
Virtual entity: Firewall – external interface
```

Example 2 : (Add an address translation rule 1-1 at the end of the table. Mapping the *SMTP Server*, with the address reserved for the *External Server*, with a valid address for all hosts from the Internet).

```
#/aker/bin/firewall/fwnat adds at the end 1-1 "SMTP Server" Internet "External Server"
Rule included at position 6
```

Example 3: (Adding a translation rule n-n at position 5).

```
#/aker/bin/firewall/fwnat adds 5 n-n network1 Internet network2.
Rule included at position 5
```

Example4 : (Adding a service translation rule at the beginning of the table).

```
#/aker/bin/firewall/fwnat adds 1 service "Server 2" Internet "External Server 2" Telnet FTP
Rule included at position 1
```

Example 5 : (Removing rule 3).

```
#/aker/bin/firewall/fwnat remove 3
Rule 5 removed
```

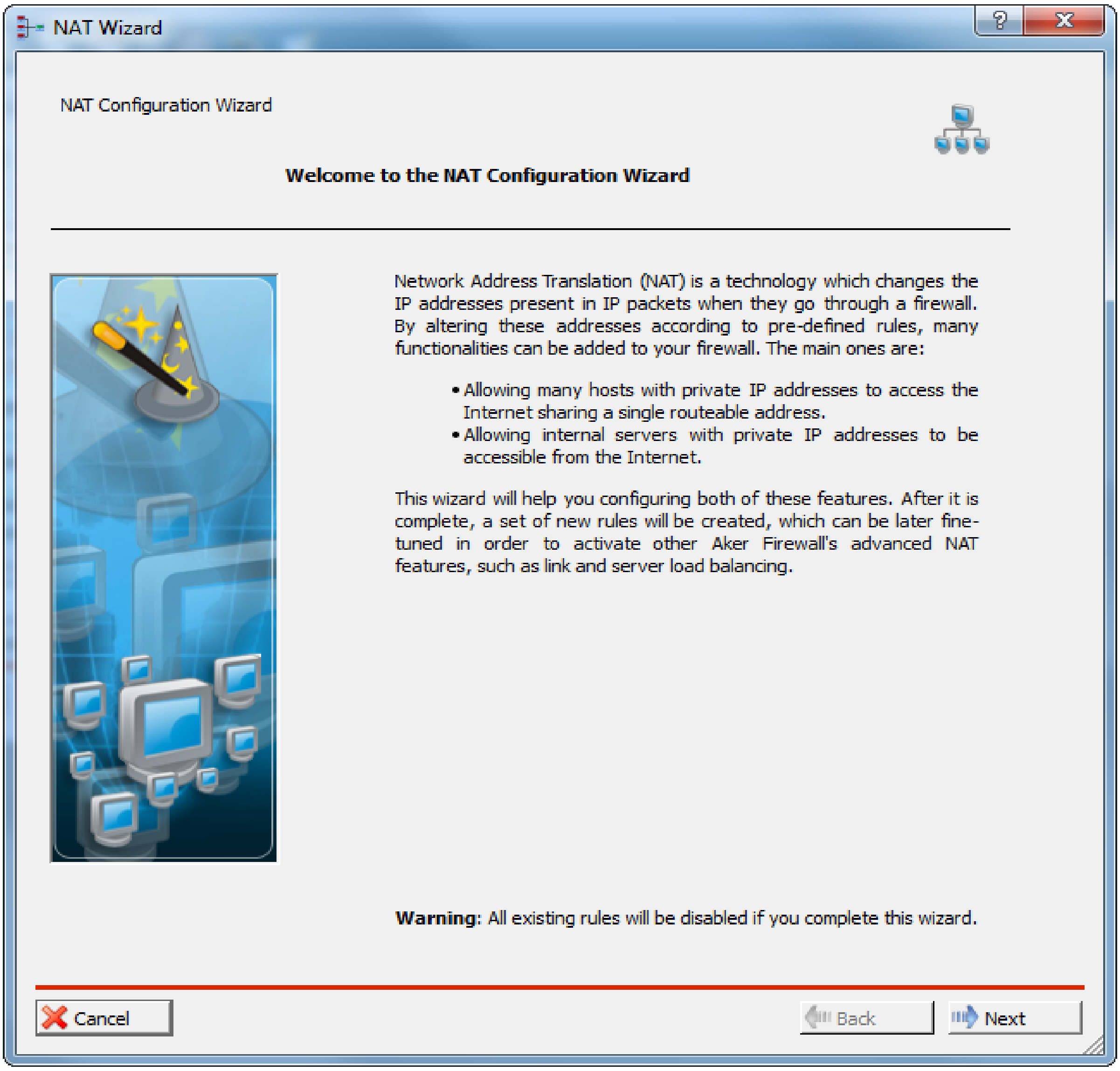
Example 6 : (Adding a rule translation 1-N, balancing, mapping the *srv01* and *srv02 servers* in an external host called *srv_external*, to all Internet hosts, and monitoring via ping).

```
#/aker/bin/firewall/fwnat adds 4 1-N srv01 srv02 Internet srv_external round-robin
ping
Rule included at position 4
```

8.3. Using the NAT configuration wizard

NAT configuration wizard can be triggered by both toolbar and menu. The windows below will describe the NAT configuration Wizard.

1 – The main window explains what is NAT. Click next to continue the configuration.



Welcome to the NAT Configuration Wizard

Network Address Translation (NAT) is a technology which changes the IP addresses present in IP packets when they go through a firewall. By altering these addresses according to pre-defined rules, many functionalities can be added to your firewall. The main ones are:

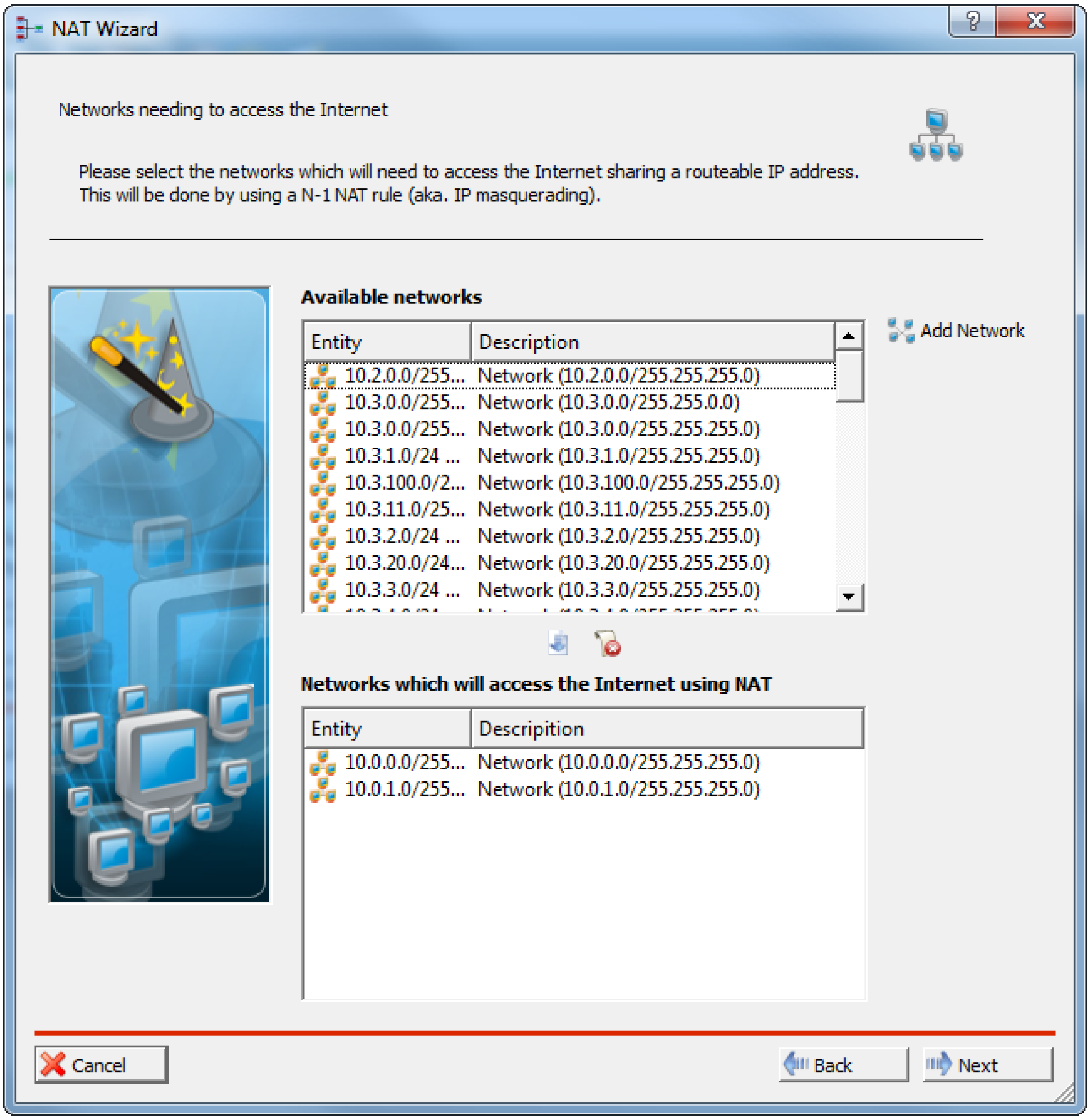
- Allowing many hosts with private IP addresses to access the Internet sharing a single routeable address.
- Allowing internal servers with private IP addresses to be accessible from the Internet.

This wizard will help you configuring both of these features. After it is complete, a set of new rules will be created, which can be later fine-tuned in order to activate other Aker Firewall's advanced NAT features, such as link and server load balancing.

Warning: All existing rules will be disabled if you complete this wizard.

Image 218 – Welcome to NAT configuration window.

2 – Choose the networks that need to access the Internet.



Networks needing to access the Internet

Please select the networks which will need to access the Internet sharing a routeable IP address.
This will be done by using a N-1 NAT rule (aka. IP masquerading).

Available networks

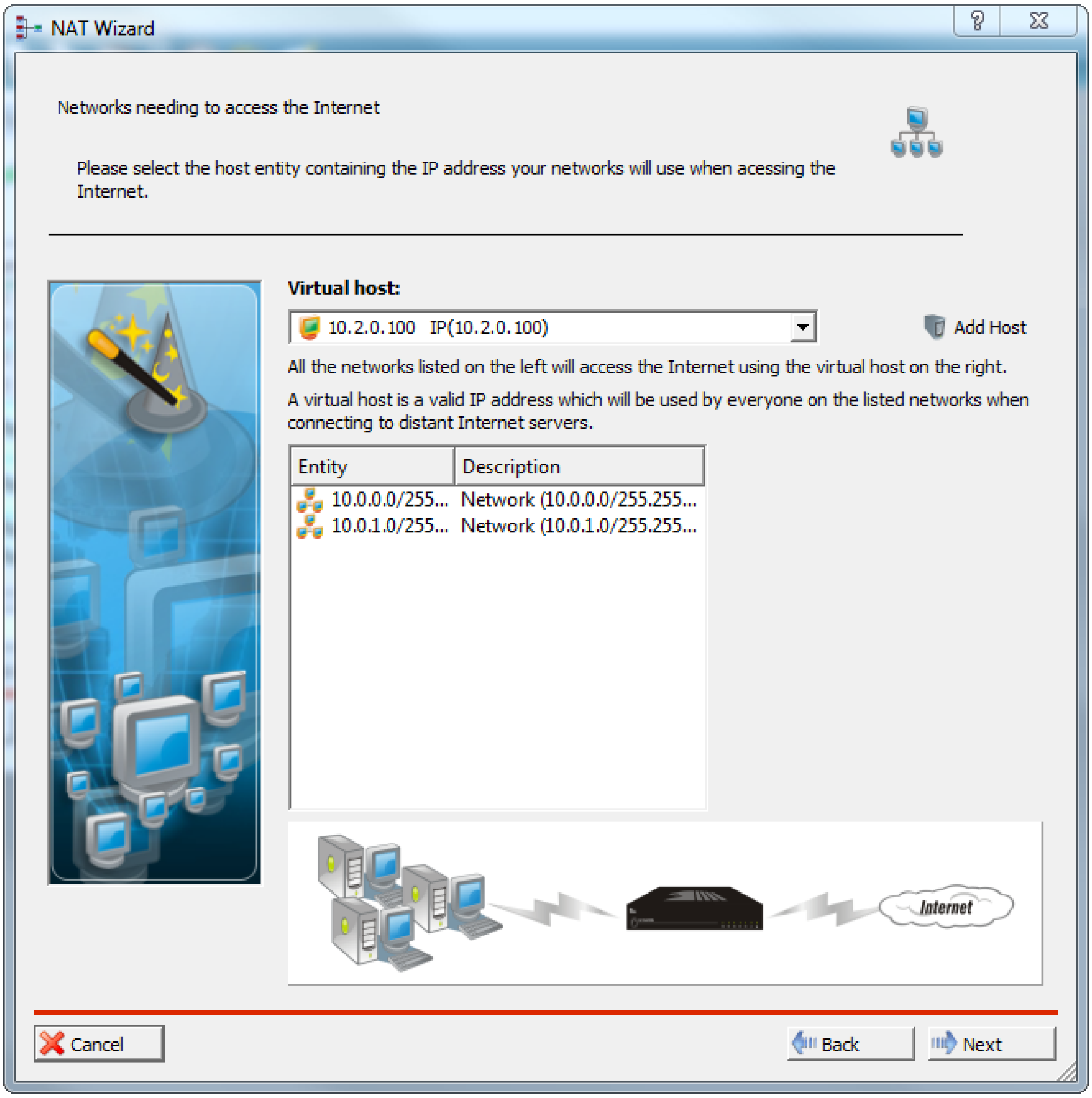
Entity	Description
10.2.0.0/255...	Network (10.2.0.0/255.255.255.0)
10.3.0.0/255...	Network (10.3.0.0/255.255.0.0)
10.3.0.0/255...	Network (10.3.0.0/255.255.255.0)
10.3.1.0/24 ...	Network (10.3.1.0/255.255.255.0)
10.3.100.0/2...	Network (10.3.100.0/255.255.255.0)
10.3.11.0/25...	Network (10.3.11.0/255.255.255.0)
10.3.2.0/24 ...	Network (10.3.2.0/255.255.255.0)
10.3.20.0/24...	Network (10.3.20.0/255.255.255.0)
10.3.3.0/24 ...	Network (10.3.3.0/255.255.255.0)

Networks which will access the Internet using NAT

Entity	Description
10.0.0.0/255...	Network (10.0.0.0/255.255.255.0)
10.0.1.0/255...	Network (10.0.1.0/255.255.255.0)

Image 219 – Selecting networks which have the need of access the Internet sharing an IP address.

3 – Choose the Virtual host IP to perform the translation N-1.



Networks needing to access the Internet

Please select the host entity containing the IP address your networks will use when acessing the Internet.

Virtual host: 10.2.0.100 IP(10.2.0.100)

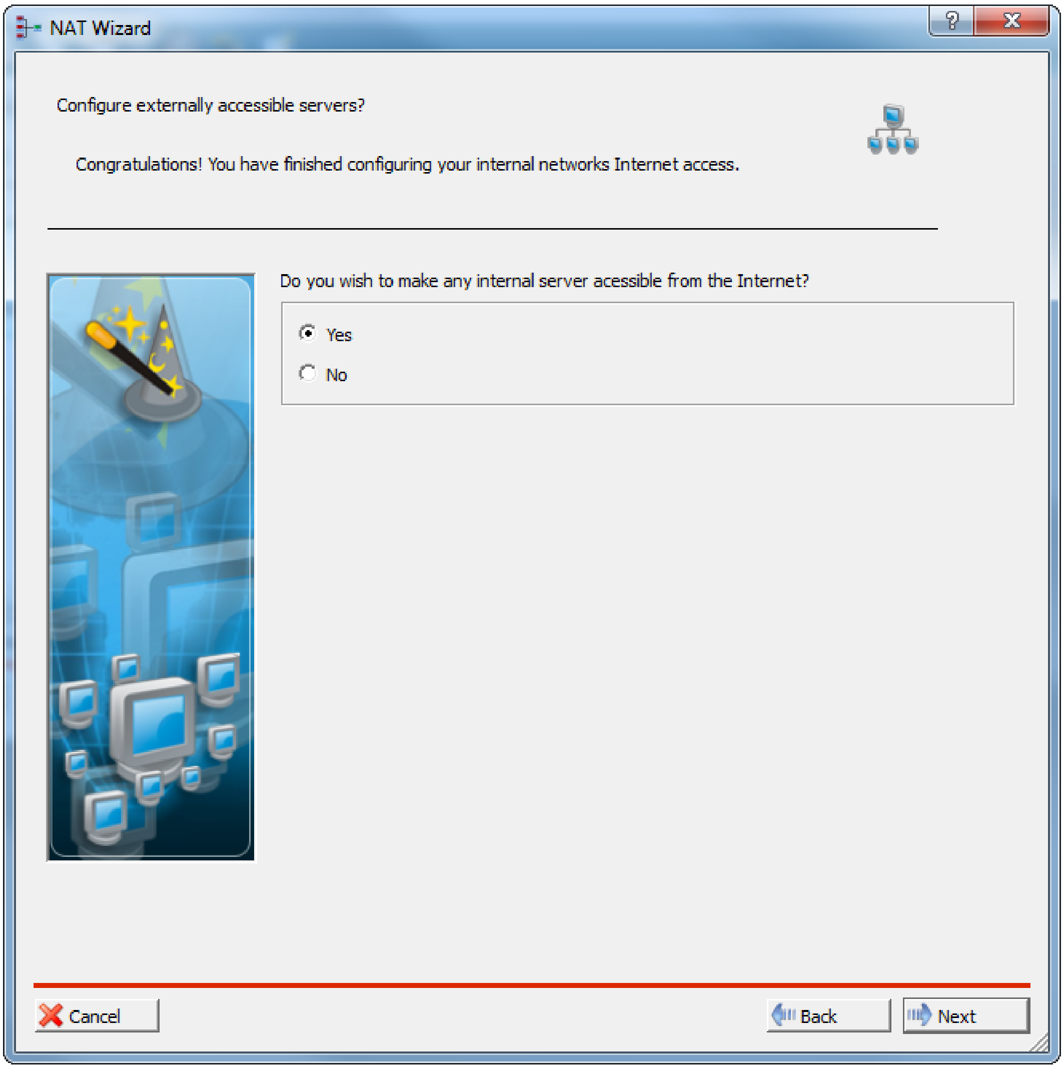
All the networks listed on the left will access the Internet using the virtual host on the right.

A virtual host is a valid IP address which will be used by everyone on the listed networks when connecting to distant Internet servers.

Entity	Description
10.0.0.0/255...	Network (10.0.0.0/255.255...
10.0.1.0/255...	Network (10.0.1.0/255.255...

Image 220 – Selecting the virtual host IP to perform the address translation N-1.

4 – Choose *YES* if you wish to configure the servers which should appear for the Internet.



Configure externally accessible servers?

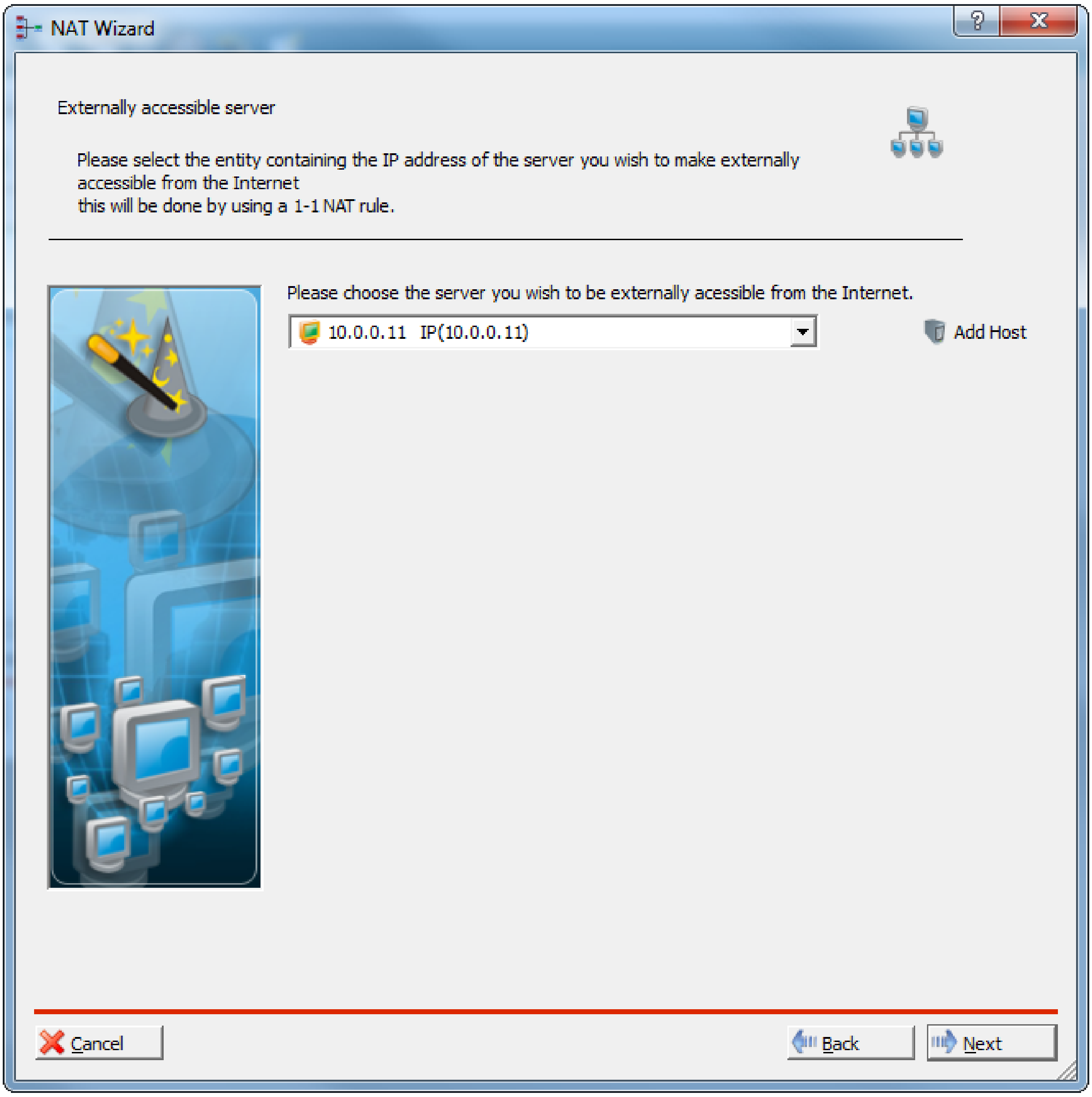
Congratulations! You have finished configuring your internal networks Internet access.

Do you wish to make any internal server acessible from the Internet?

● Yes
○ No

Image 221 – Configuring externally accessible servers.

5 – Choosing the entity to be externally accessible from the Internet.



Externally accessible server

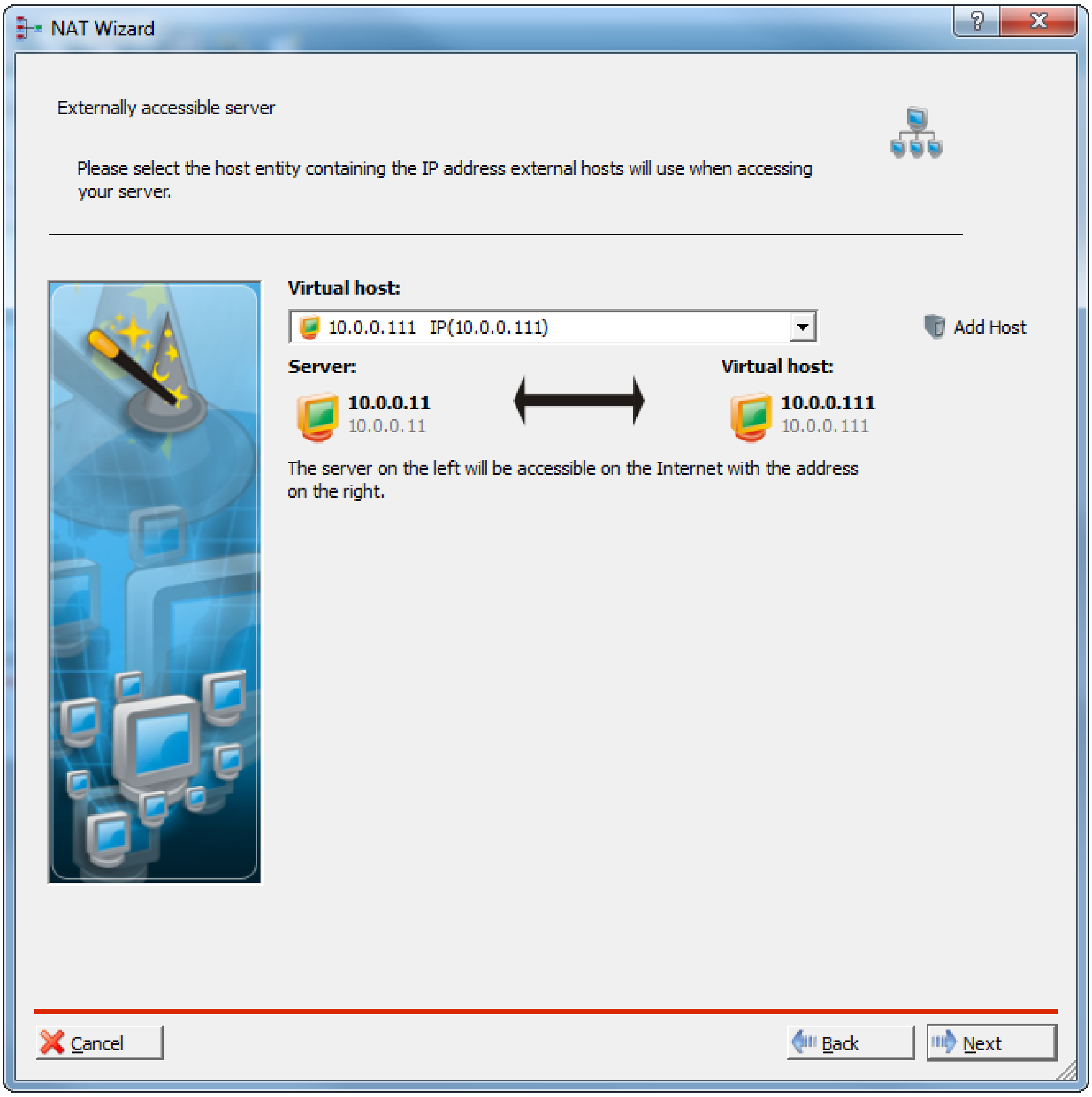
Please select the entity containing the IP address of the server you wish to make externally accessible from the Internet
this will be done by using a 1-1 NAT rule.

Please choose the server you wish to be externally acessible from the Internet.

10.0.0.11 IP(10.0.0.11)

Image 222 – Choosing the entity to be externally accessible from the Internet

6 – Choosing the Virtual Host IP which will be displayed for the Internet.



Externally accessible server

Please select the host entity containing the IP address external hosts will use when accessing your server.

Virtual host: 10.0.0.111 IP(10.0.0.111)

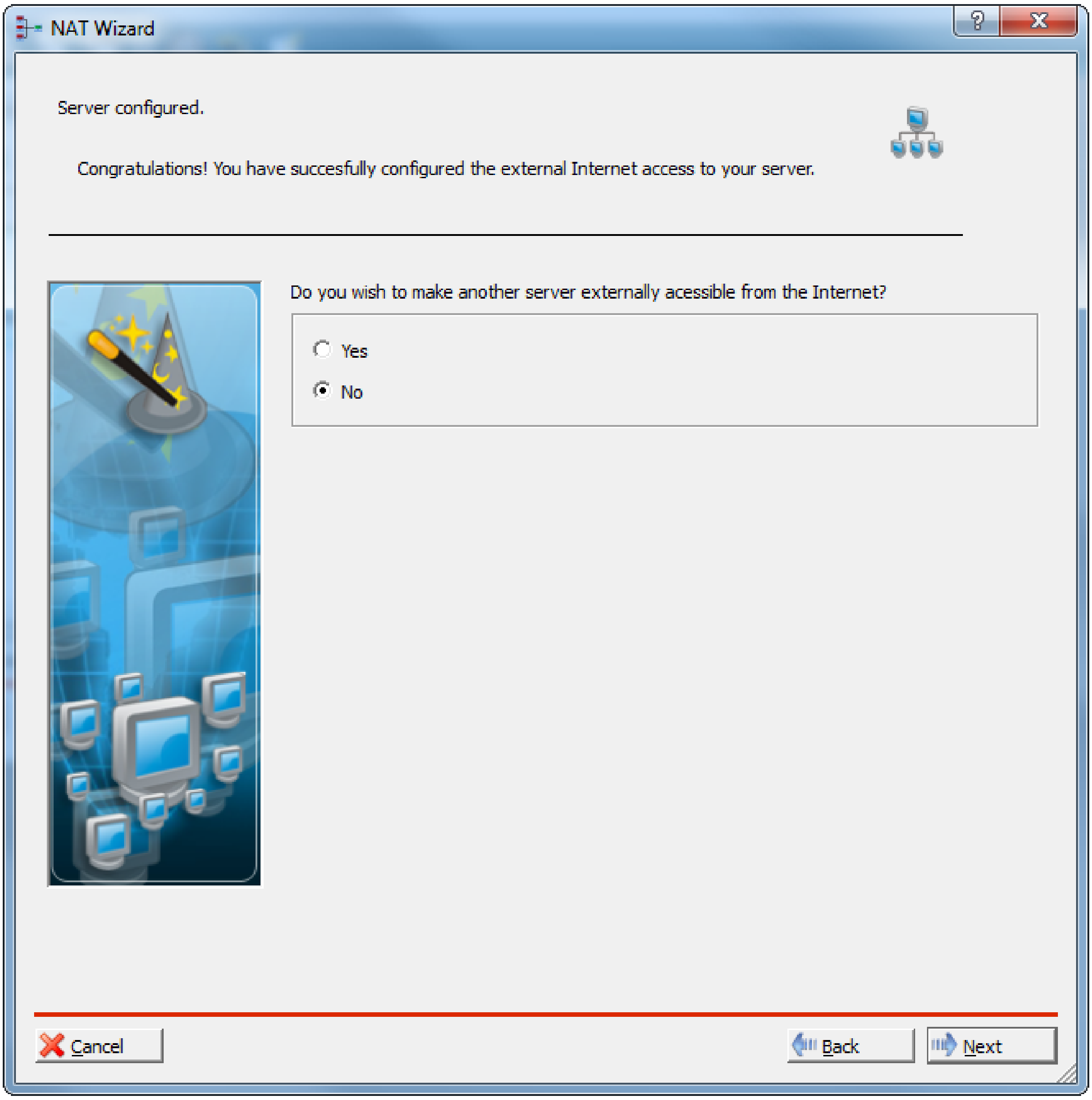
Server: 10.0.0.11 10.0.0.11

Virtual host: 10.0.0.111 10.0.0.111

The server on the left will be accessible on the Internet with the address on the right.

Image 223 – Choose the IP address used by external host, which will be used in the server.

7 – This screen will allow the configuration of more servers.



Server configured.

Congratulations! You have succesfully configured the external Internet access to your server.

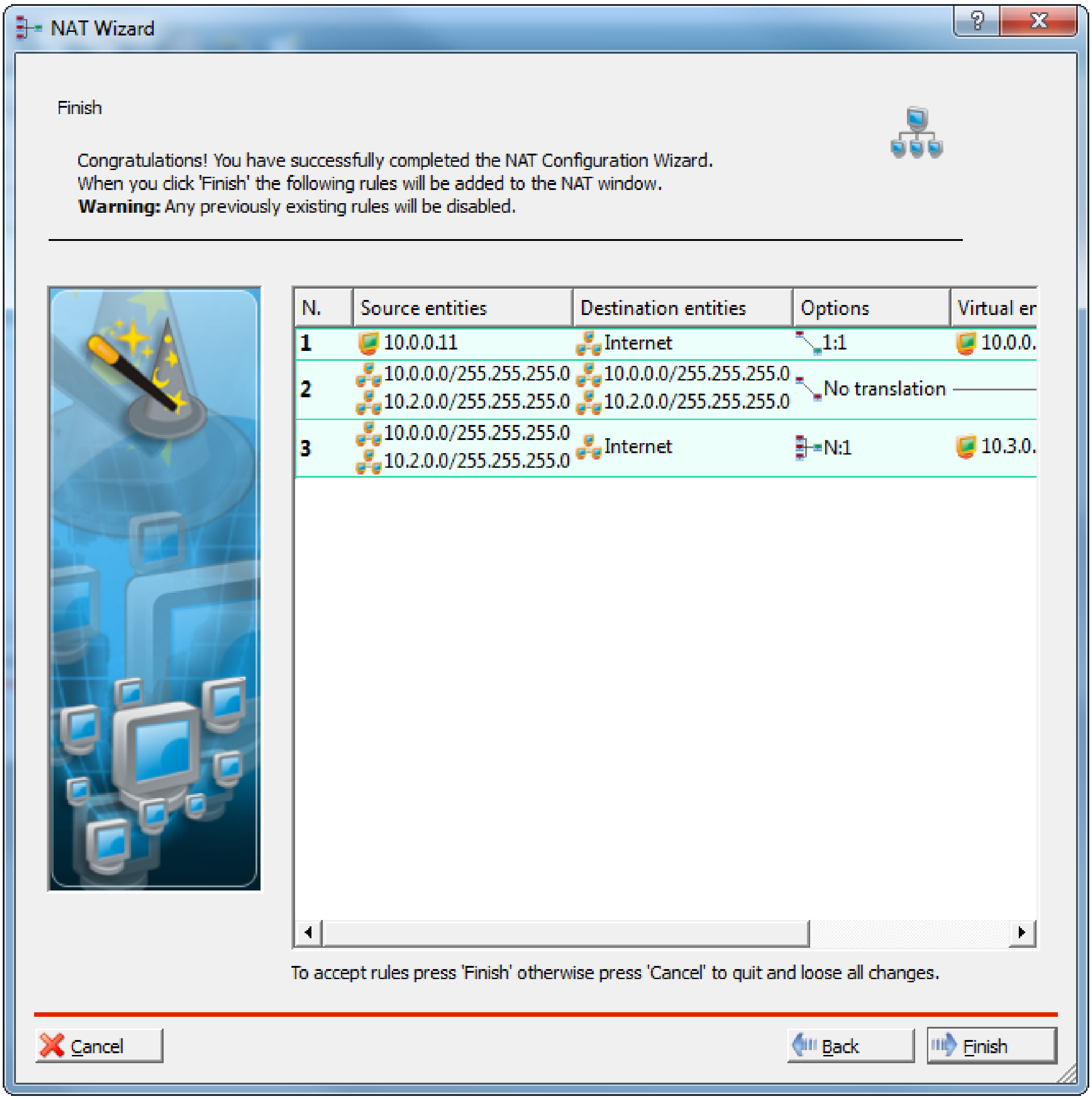
Do you wish to make another server externally acessible from the Internet?

○ Yes

● No

Image 224 – Choosing the configuration of more servers.

8 – NAT Wizard finish window.



Finish

Congratulations! You have successfully completed the NAT Configuration Wizard.
When you click 'Finish' the following rules will be added to the NAT window.
Warning: Any previously existing rules will be disabled.

N.	Source entities	Destination entities	Options	Virtual er
1	10.0.0.11	Internet	1:1	10.0.0.
2	10.0.0.0/255.255.255.0 10.2.0.0/255.255.255.0	10.0.0.0/255.255.255.0 10.2.0.0/255.255.255.0	No translation	
3	10.0.0.0/255.255.255.0 10.2.0.0/255.255.255.0	Internet	N:1	10.3.0.

To accept rules press 'Finish' otherwise press 'Cancel' to quit and loose all changes.

Image 225 – NAT wizard finish window

Creating encryption channels

9. Creating encryption channel

This chapter shows how to configure the rules which will assist in the creation of secure communication channels in the Internet. These secure channels are used to connect the institutions through the Internet allowing the data flow among them without the risk of this data be read or changed by unauthorized users.

9.1. Nat Traversal (NAT-T)

NAT traversal is a general term for techniques that establish and maintain Internet protocol connections traversing network address translation (NAT) gateways. Network address translation breaks end-to-end connectivity. Intercepting and modifying traffic can only be performed transparently in the absence of secure encryption and authentication. NAT traversal techniques are typically required for client-to-client networking applications, especially peer-to-peer and Voice over IP (VoIP) deployments. Many techniques exist, but no single method works in every situation since NAT behavior is not standardized. Many NAT traversal techniques require assistance from a server at a publicly routable IP address. Some methods use the server only when establishing the connection, while others are based on relaying all data through it, which adds bandwidth costs and increases latency, detrimental to real-time voice and video communications.

Most NAT behavior-based techniques bypass enterprise security policies. Enterprise security experts prefer techniques that explicitly cooperate with NAT and firewalls, allowing NAT traversal while still enabling marshalling at the NAT to enforce enterprise security policies. From this point of view, the most promising IETF standards are Realm-Specific IP (RSIP) and Middlebox Communications (MIDCOM).

SOCKS, the oldest NAT traversal protocol still widely available. In home or small office settings, Universal Plug and Play (UPnP) is supported by most small NAT gateways. NAT-T is commonly used by IPsec virtual private network clients in order to have Encapsulating Security Payload packets traverse NAT.

Aker Firewall detects automatically the need of using the NAT transversal for the tunnel establishment.

In order to deactivate the use of NAT traversal in Aker Firewall it is necessary to start the daemon “fwiked” with **: "aker/bin/firewall/fwiked-T"**.

9.2. Planning installation

What is a secure data channel and what is it using?

The Internet is a worldwide network composed by thousands of hosts spread all around the world. When two computers are communicating with each other, all traffic between them passes through several other hosts (routers, switches, etc.) from its source to its destination.

Any of these computers which are in the path of packets can visualize its content or change it. It is a serious problem, and its importance increases even more when there is a need of transmitting *confidential data* and data of *huge impact*.

To solve this problem, you can use a secure data channel. A secure data channel can be seen as a tunnel. From one side the information is placed, information which will be available for reading after exiting the other side of the tunnel.

The data that will be transmitted are given a special treatment, in order to protect these data from changing or visualizing during its transmission (authentication and encryption). The combination of these two techniques produces invisible and immutable data for any hosts which are located in the path of packets, from source to destination.

What is encryption?

In cryptography, *encryption* (also known as the combination of a key with a mathematical algorithm based on a *one-way function*) is the process of transforming information (referred to as plain-text) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). The reverse process, i.e., to make the *encrypted* information readable again, is referred to as *decryption* (i.e., to make it *unencrypted*).

In many contexts, the word encryption may also refer to the reverse process, *decryption* e.g. “software for encryption” can typically also perform decryption.

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized *encryption* for some of their data in transit, and 53% utilized *encryption* for some of their data in storage.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller hosts. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it, as it is often difficult to physically secure all access to networks

What is authentication?

Authentication is the combination of a key with a mathematical algorithm based on a *one-way function* as well. The difference between authentication and encryption is; when applied authentication on the data, it does not make the data unreadable instead it creates a *digital signature* for it.

When the digital signature is generated, it starts to be transmitted to the destination together with the data. In case the data have suffered any changes in its way, the receiver when calculating the *digital signature* from the received data and compare it to the original signature will realize the data has been changed.

Authentication is an operation quite fast when compared to encryption, but authentication alone cannot stop the data from being read. It should be used only if there is a need of reliability of data, but not secrecy. In case you need both, authentication and encryption shall be used together.

What is a digital certification?

The Digital Certification is the identity of individuals and companies in the electronics environment, allowing their users perform secure and reliable transactions **.**Through the *authentication process* described above it is possible to ensure origin of messages in a communication between two parts. However to make it possible it is necessary the entities that are communication with each other, have already exchanged information through any mean, not being in the regular data traffic. This exchange of information normally consists in the algorithm used for the authentication and its key.

The problem is when it is necessary to ensure the source of messages of an entity which has never been connected to the target entity. The only way to solve this problem is delegate a third entity the right to perform these authentications (perform a source of messages certification). This third entity is called ***Certified Entities,*** in order to ensure the source of a message; it must to have performed an exchange of information with the entity which is being certified.

What is a digital certificate?

In cryptography, a *public key certificate* (also known as a *digital certificate* or *identity certificate*) is an electronic document which uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

Authentication and encryption types of algorithm

Nowadays there are numerous encryption and authentication algorithms. In this topic is presented only the algorithms supported by Aker Firewall.

It is worth mentioning that one of the parameters to measure the resistance of an algorithm is its key's size. As larger the keys *bits* number, larger will be the number of possible combinations, theoretically, greater will be the algorithm resistance against attacks.

Authentication algorithm:

- **MD5**

  The *MD5 Message-Digest Algorithm* is a widely used cryptographic hash function that produces a *128-bit (16-byte)* hash value. Specified in RFC 1321, *MD5* has been employed in a wide variety of security applications, and is also commonly used to check data integrity. *MD5* was designed by *Ron Rivest* in 1991 to replace an earlier hash function, *MD4*. An *MD5* hash is typically expressed as a hexadecimal number, 32 digits long.

  SHA

  The *Secure Hash Algorithm* is one of a number of cryptographic hash functions published by the *National Institute of Standards and Technology (NIST*) as a U.S. *Federal Information Processing Standard (FIPS): SHA* is an algorithm that generates digital signatures of *160 bits* for messages of any size. It is also considered safer than MD5.

  The version implemented by Aker Firewall is *SHA-1. It is* a 160-bit hash function which resembles the earlier MD5 algorithm. SHA-1 will always be called SHA in this manual and in the administration interfaces.

Symmetrical encryption algorithm:

Symmetrical encryption algorithms are used to encrypt information flows. It has a single key which is used to encrypt and decrypt data.

- **DES**

  Developed in the early 1970s at IBM and based on an earlier design by *Horst Feistel*, *DES (DATA ENCRYPTION STANDARD)* is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm, a number considered small nowadays. Due to it, it is preferable the use of other algorithm in case of critical application.

- **Triple DES or 3DES**

Triple DES is the common name for the *Triple Data Encryption Algorithm (TDEA or Triple DEA)* block cipher, which applies the *Data Encryption Standard (DES)* cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits (key sizes 168, 112 or 56 bits) was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. The only problem is that the 3DES is twice slower than DES (in the implementation used in Aker Firewall).

- **AES**

The Advanced *Encryption Standard (AES)* is a specification for the encryption of electronic data. Originally called *Rijndael*, *AES* has been adopted by the U.S. government and is now used worldwide. It supersedes the *Data Encryption Standard (DES)*. The algorithm described by *AES* is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Aker Firewall works with AES using Keys of 256 bits, which ensure a high level of security. It is the recommended choice.

- **Blowfish**

  Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes. Blowfish is extremely fast when compared to other encryption algorithm.

Aker Firewall works with Blowfish using Keys of 128 or 256 bits, which ensure a high level of security.

Asymmetric encryption algorithms:

Asymmetric encryption algorithms have a pair of Keys assigned one to encrypt and the other to decrypt the data. There are really slow compared to the symmetrical algorithms, due to it, they are normally used to make digital signatures and establishing session keys which will be used in the symmetrical algorithms.

- **RSA**

  RSA is an algorithm based in the modular arithmetic capable of working with keys of any size, but values lower than 512 bits are considered very fragile. It can be used to encrypt and decrypt data, due to its slowness compared to the symmetrical algorithms; its main use is for digital signatures and establishing session keys.

- **Diffie-Hellman**

  Diffie–Hellman key exchange (D–H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. It is also based in the modular arithmetic capable of working with keys of any size, but values lower than 512 bits are considered very fragile.

Key Exchange algorithms

A basic problem that occurs when you configure a secure channel is how to configure the encryption and authentication keys and how to make periodic exchanges of these keys.

It is important to make periodic exchanges of keys in order to reduce the possibility of a key breaking by a hacker and to reduce the damage in case this attacker is able to decipher one of the keys. Let us suppose a hacker breaks a key used by an encryption algorithm in six months. If the company uses the same key during a year, then, the hacker will decipher all traffic from the last 6 months of this company’s network. However, if the key is exchanged daily, the hacker after 6 months will decipher the traffic from the first day, and will take 6 more months to decipher the traffic of the second day and so on.

Aker Firewall has four exchange methods: IPSEC-IKE, AKER-CDP, SKIP and manual:

- **Key exchange via IPSEC-IKE**

  This option will be available only when the complete set of IPSEC protocol be used.

  IPSEC (*IP Security*) is a set of standardized protocols (RFC 2401- RFC 2412) developed by IETF. IPSEC offers secure transfer of information through public or private IP network. A connection through IPSEC always involves 3 steps:

  1. Security level negotiation;
  2. Authentication and Integrity;
  3. Confidentiality.

  To implement these 3 steps IPSEC uses 3 mechanisms:

  AH – Authentication Header
  ESP – Encapsulation Security Payload
  IKE – Internet Key Exchange Protocol

  It is strongly recommended the use of this option when configuring the secure channels.

- **Key Exchange via Aker-CDP**

  Aker-CDP is a protocol developed by Aker Security Solutions that make possible fully automatic configuration of all parameters of a secure channel. It uses the protocol SKIP as base (meaning it offers all the key exchange facilities presented above), it has a great advantage which is; there is no need to configure the *shared secrets manual,* everything is done automatically.

  To ensure maximum protection, every key Exchange is made through digital certificate signed by Aker or by other authorized certified entities. In these certificates are used Diffie-Hellman and RSA, both with 1025 bits.

  The algorithm used in the encryption and authentication can be specified in the same way as the SKIP protocol, or left in automatic mode, which will make the two communicating firewall negotiate the most secure algorithm for both.

- **Key Exchange via SKIP**

  SKIP is an anagram for *Simple Key Management for IP*. Basically it is an algorithm that allows the key exchange be performed automatically and with an extremely high frequency, making it unfeasible to break these keys.
  Basically SKIP works with three different types of keys:

  - A secret shared by the two entities that wish to communicate (manually configured, for Aker Firewall).
  - A master key, recalculated hourly, based in the shared secret.
  - A random key that can be recalculated whenever you want.

To perform a communication, the algorithm generates a random key and the key used to encrypt and authenticate the selected data to be sent. Then it encrypts this master key and sends it together with the encrypted data. By receiving the packet, the other side decrypts the key, assisted by the master key, and uses it to decrypt the rest of the packet.

The algorithm used to authenticate the packet and encrypt the key are defined by the sender and reported as part of the protocol. This way, it is not necessary configuring these parameters in the receiver.

The main advantage of SKIP is the possibility of using the same shared secret for years, without any risk of any hacker break the keys (once the key exchange is performed in few seconds interval or at maximum in an hour, depending in the traffic between the communicating networks).

- **Manual key exchange**

In this case, all keys configuration will be made manually. This means every time a key is exchanged, both participating firewalls of a secure channel will have to be reconfigured simultaneously.

Types of secure channels

Aker Firewall allows the creation of two distinct types of secure channels, called Firewall-Firewall and Client- Firewall. Each of these channels has different objectives and limitations and normally they are combined in order to reach the maximum security and flexibility.

- ***Firewall-Firewall* secure channel**

This is the most common type of secure channel supported by Aker Firewall since its version 1.31. It consists in the use of encryption and authentication between two firewalls, connected through the Internet or any other mean. The channel *entry* and *exit points* are the two firewalls, which means all encryption is done transparently by them and no additional software need to be installed in any client host.

The only limitation of this solution is that it requires the presence of two firewalls, one in the entry of each network, in order to create the secure channel.

- ***Client-Firewall* secure channel (Secure Roaming)**

These channels are supported by Aker Firewall from version 3.10. They allow the host client (Windows and Linux) to establish a secure channel directly with an

Aker Firewall. Therefore, it is necessary installing a program called Aker Client, in each one of these computers.

The main advantage of this technology is; allow the clients to access the corporate network via dial-up lines with total security and transparency.

Aker Client is an authenticator that allows clients to access the corporate network with total security and transparency, establishing secure channels between clients and firewall.

Despite being quite useful this technology has few disadvantages and limitations:

- It is necessary to install *Aker Client*, in all client hosts;
- The encryption client is not available to all platforms;

Defining a secure channel firewall-firewall

To define a *Firewall-firewall secure channel* first you must to choose two hosts group which will exchange information between themselves in a secure way. These hosts groups will have their packets authenticated and encrypted if desired. There must to be a firewall on both channels. These firewalls will be responsible to authenticate/verify/ encrypt and decrypt the data selected be transmitted and received.

To define the hosts groups, an entity concept will be used, displayed in the chapter titled ***Registering Entities.*** Entities type: host, network or set in this definition can be used.

Aker Firewall supports the existence of several secure channels simultaneous, between distinct points. The unions of these several channel create a list, where each entry defines completely the parameters of a secure channel. Each one of these entries receive the name SA (Security association)

The planning of these secure channels shall be done very carefully. The encryption is an expensive resource that demands a high capacity of processing. This way, encrypting packets which there are no real need of security, will be a waste of resource. Besides it, must to pay attention because different encryption algorithms require different amounts of processing, and produce a higher level of security. Depending on the desired level of security, you may choose different algorithm (the description of Aker Firewall for each supported algorithm, is present in the previous topic).

A last note about the encryption channel *Firewall-Firewall* is that they are unidirectional, i.e., if you desire to configure a secure communication between two networks, A and B for example, you must to configure two different channels: a channel with source in network A and destination in network B, and other with the source in network B and destination in network A. the packets which have been sent from A to B will follow the configuration of the first channel, and packets from B to A will follow the configuration of the second channel. This will be illustrated clearly in the example bellow:

Examples of Firewall-firewall secure channel use

This example shows how to define a secure channel of information, between two networks, through the Internet, using two Aker Firewalls. The Channel will be created so all communication between these two networks be secured. MD5 has been chosen to be the authentication algorithm and DES as the encryption algorithm.

It is mandatory the use of one authentication algorithm for all flows, i.e., it is not allowed the creation of flows with encryption only. This is necessary since without the authentication the encryption algorithms are vulnerable to *cut and paste* attacks.

- **Network 1 Aker Firewall configuration**

Entities:

NETWORK1 – IP Address: **A1.B1.C1.0 –** Mask **255.255.255.0**
NETWORK 2 – IP Address: **A2.B2.C2.0 –** Mask **255.255.255.0**

Encryption rule 1:

Channel direction: **send**
Source entities: **NETWORK1**
Destination entities: **NETWORK 2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Encryption rule 2:

Channel direction: **receive**
Source entities: **NETWORK2**
Destination entities: **NETWORK1**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X3**
Encryption key: **X4**

- **Network 2 Aker Firewall configuration**

Entities:

NETWORK1 – IP Address: **A1.B1.C1.0 –** Mask **255.255.255.0**
NETWORK2 – IP Addresses: **A2.B2.C2.0 –** Mask **255.255.255.0**

Encryption rule 1:

Channel direction: **receive**
Source entities: **NETWORK1**
Destination entities: **NETWORK2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Encryption rule2:

Channel direction: **send**
Source entities: **NETWORK2**
Destination entities: **NETWORK1**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X3**
Encryption key: **X4**

Take note that rule from Aker Firewall 1 is exactly the same as rule 1 from Aker Firewall 2, except for the field *CHANNEL DIRECTION*. The same applies to rules 2.

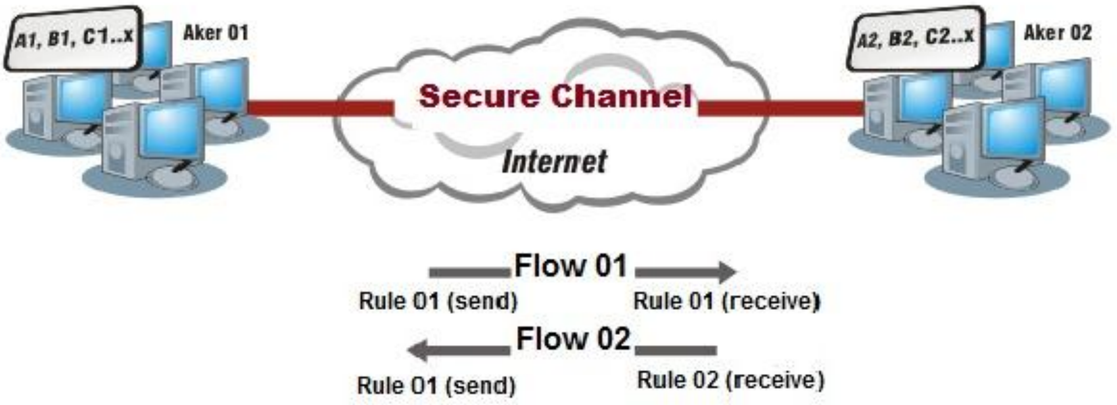

A1, B1, C1..x
Aker 01
Secure Channel
Internet
A2, B2, C2..x
Aker 02
Flow 01
Rule 01 (send)
Rule 01 (receive)
Flow 02
Rule 01 (send)
Rule 02 (receive)

Image 226 – Configuration of a Secure Channel Firewall-firewall to a sub network.

Example of a Firewall-firewall secure channel configuration for a subnetwork

In this example our secure channel will be defined only for a group of hosts within each one of the two networks. Besides it, we will define different algorithms for the flows among these groups.

In this example, let us assume that the networks 1 and 2 have two class B addresses: A1.B1.0.0 and A2.B2.0.0, respectively.

- **Network 1 Aker Firewall configuration**

Entities:

SUBNETWORK1 – IP Address: **A1.B1.2.0 –** Mask **255.255.255.0**
SUBNETWORK2 – IP Address: **A2.B2.5.0 –** Mask **255.255.255.0**

Encryption rule 1:

Channel direction: **send**
Entidades origem: **SUBNETWORK1**
Entidades destino: **SUBNETWORK2**
Algoritmo de criptografia: **DES**
Algoritmo de autenticação: **MD5**
Chave de autenticação: **X1**
Chave de criptografia: **X2**

Encryption rule 2:

Channel direction: **receive**
Source entities: **SUB_REDE2**
Destination entities: **SUB_REDE1**
Encryption algorithm: **3DES**
Authentication algorithm: **SHA**
Authentication key: **X3**
Encryption key: **X4**

- **Network 2 Aker Firewall configuration**

Entities:

SUBNETWORK1 – IP Address: **A1.B1.2.0 –** Mask **255.255.255.0**
SUBNETWORK2 – IP Address: **A2.B2.5.0 –** Mask **255.255.255.0**

Encryption rule 1:

Channel direction: **send**
Source entities: **SUBNETWORK 2**
Destination entities: **SUBNETWORK 1**
Encryption key: **3DES**
Authentication algorithm: **SHA**
Authentication key: **X3**
Encryption key: **X4**

Encryption rule 2:

Channel direction: **receive**
Source entities: **SUBNETWORK1**
Destination entities: **SUBNETWORK2**
Encryption Algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Notice that in this case the secure channels appear in a different order in the two firewalls: rule 1 in the Firewall 1 is the same as rule 2 in the Firewall 2 (with inverted directions) and rule 2 in the Firewall 1 is the same as rule 1 in the Firewall 2 (again with inverted directions). In this example, the order of the rules does not make any difference (notice, however, that in some cases this cannot be true)

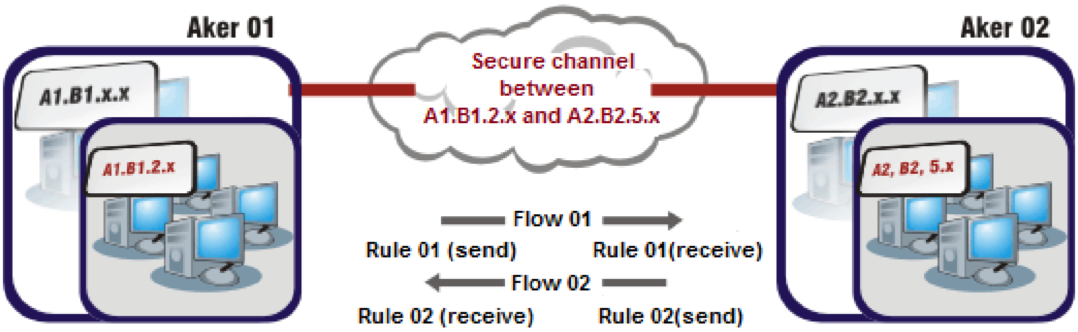

Aker 01
A1.B1.x.x
A1.B1.2.x
Secure channel
between
A1.B1.2.x and A2.B2.5.x
Aker 02
A2.B2.x.x
A2, B2, 5.x
Flow 01
Rule 01 (send)
Rule 01(receive)
Flow 02
Rule 02 (receive)
Rule 02(send)

Image 227 – Secure channel between networks.

IPSEC certificates

IPSEC certificates follow X.509 standard. They are used by a firewall to identify itself to another firewall, when establishing encrypted Firewall-firewall channels, in IPSEC standard (see section below *Configuring IPSEC tunnels*). Their use, however, is not mandatory, since it is possible to establish an IPSEC tunnel by authenticating both parties using shared secrets.

To accept firewall certificates, a firewall must also have a certificate issued by the same Certification Authority.

To access the window IPSEC certificate maintenance, follow the steps bellow:

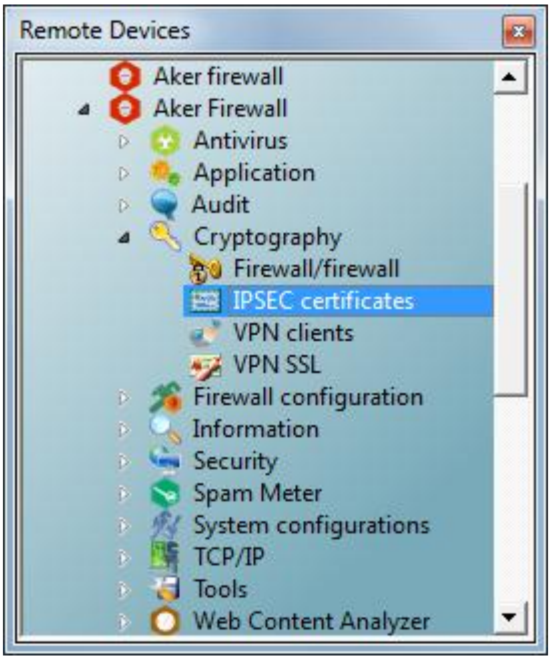

Remote Devices
Aker firewall
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall/firewall
IPSEC certificates
VPN clients
VPN SSL
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 228 – Remote Devices (IPSEC certificates).

- Click on *Cryptography menu* in the main window.
- Choose *IPSEC certificates*.

The IPSEC certificates and requests windows

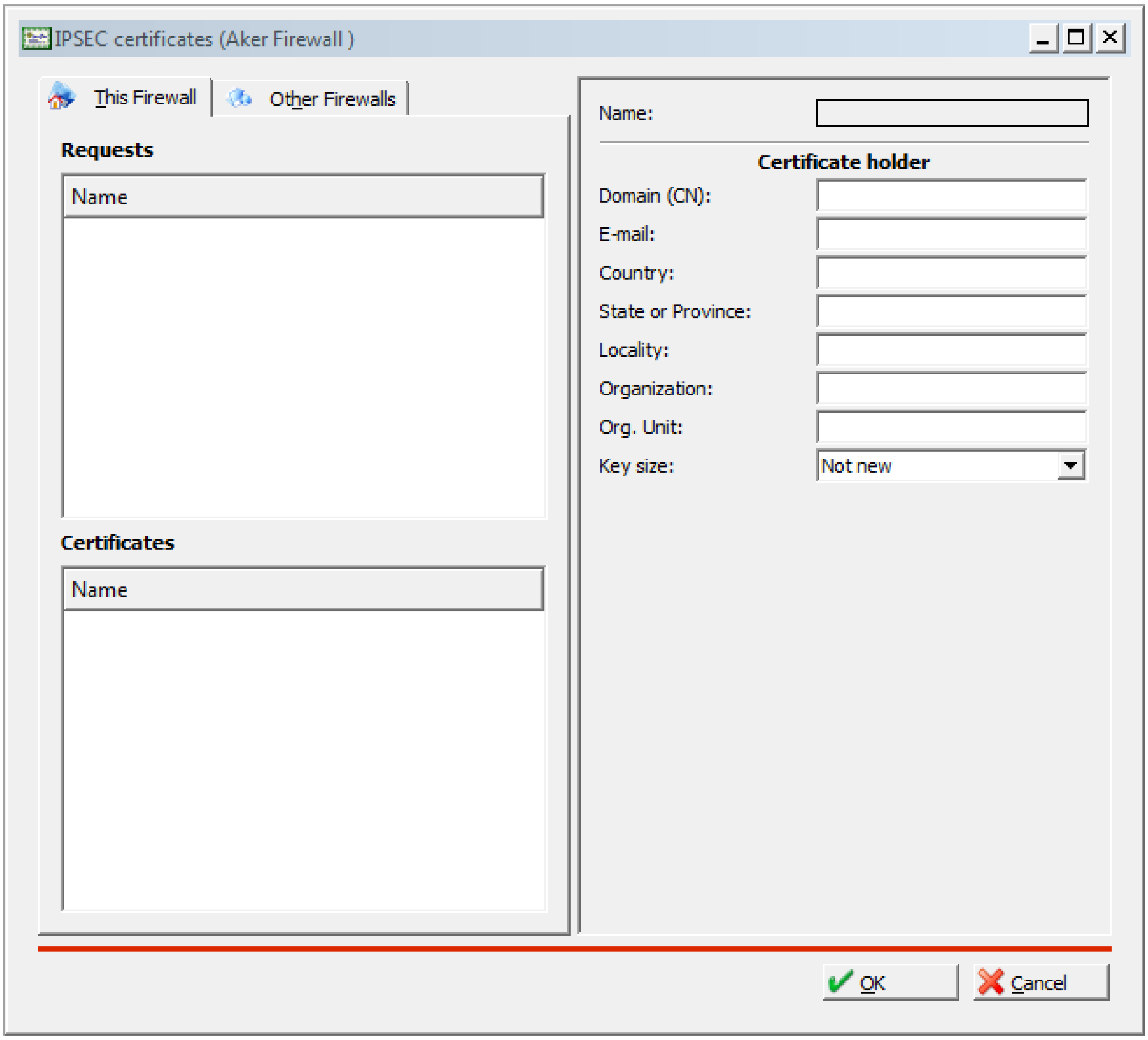

IPSEC certificates (Aker Firewall)
This Firewall
Other Firewalls
Requests
Name
Certificates
Name
Name:
Certificate holder
Domain (CN):
E-mail:
Country:
State or Province:
Locality:
Organization:
Org. Unit:
Key size:
Not new
OK
Cancel

Image 229 – IPSEC certificates window.

The IPSEC Certificates window contains Aker Firewall certificates and requests.

A request is a form to be filled with your data so that the Certification Authority can issue a certificate. A certificate is an ID card to guarantee the owner really is who he/she claims to be. When negotiating an IPSEC channel with other firewall, Aker Firewall uses these certificates to identify itself to the other firewalls. Thus, both firewalls, involved in an IPSEC firewall-firewall channel, have to generate their own certificate.

This window operation can be found in the toolbar above the IPSEC Certificates window, or by right-clicking over the desired field

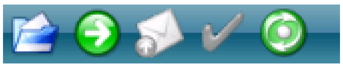


Image 230 – Toolbar (IPSEC certificates).

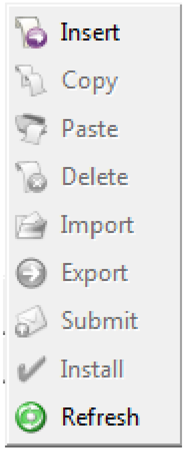


Image 231 – *IPSEC certificates* action window.

- The ***INSERT*** button allows to add a new request, it can be *Local* or *Remote* (the *Local* requests and certifications will be found in this firewall windows, and the *Remote* requests and certifications will be found in other firewall windows.
- The ***COPY*** button copies the selected certificate/ request.
- The ***PASTE*** button pastes the certificate/request copied.
- The ***DELETE*** button removes the selected certificate/request from the list.
- The ***IMPORT*** button allows loading a certificate which has been exported.
- The ***EXPORT*** button allows saving the selected certificate.
- The **SUBMIT** button allows loading an exported certificate or load a certificate according to the selected request (it will only appear when you are adding a new certificate).
- The **INSTALL** button will update and close the window.
- The **REFRESH** button reloads the certificate information.

Before generating a certificate, it is first necessary to generate a request in Aker Firewall. With this request, ask a Certification Authority to generate the certificate. Then, import it to the Aker Firewall.

This window is dynamically updated, i.e., it is not possible to cancel a submitted request. When inserting a new local request, local requests and certificates will be deleted. The same will happen to them, when importing a new local certificate with pair of keys (.pfx).

Therefore, the operation occurs as follows (for a local certificate):

1. Create a local request.
2. Send this request to a Certification Authority
3. Wait until the Certification Authority issues and returns the corresponding certificate
4. Load the certificate (click on Request, then on Load)

The procedure is different to create a certificate for a remote firewall:

1. Create a remote request.
2. Send this request to a Certification Authority.
3. Wait until the Certification Authority replies with the corresponding certificate.
4. Load the certificate (click on Request, then on Load)
5. Export/save the certificate to/in a PKCS#12 file (click on the remote certificate, and then, on Export)
6. Import this certificate in the remote firewall, selecting *This Firewall*, and then, right-clicking on *Import*.

In the request window, there are two fields that may be confusing:

- **Domain (CN):** It is the main identifier of the request owner. This field must be filled with the *common name.*
- **Key size:** If the certificate is remote, or local with the creation of a new key, this field will store the key size in bits. Otherwise (additional local certificate), this field may not be modified, once the existing key will be used.

Configuring Firewall-Firewall channels

To gain access to the Firewall-Firewall channel configuration window, please follow the steps bellow:

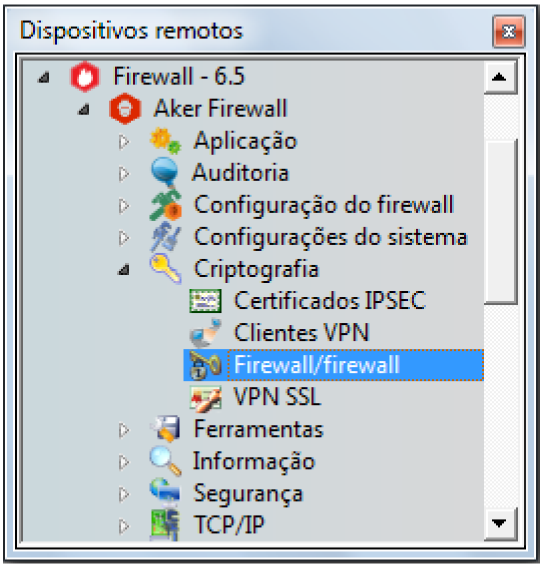
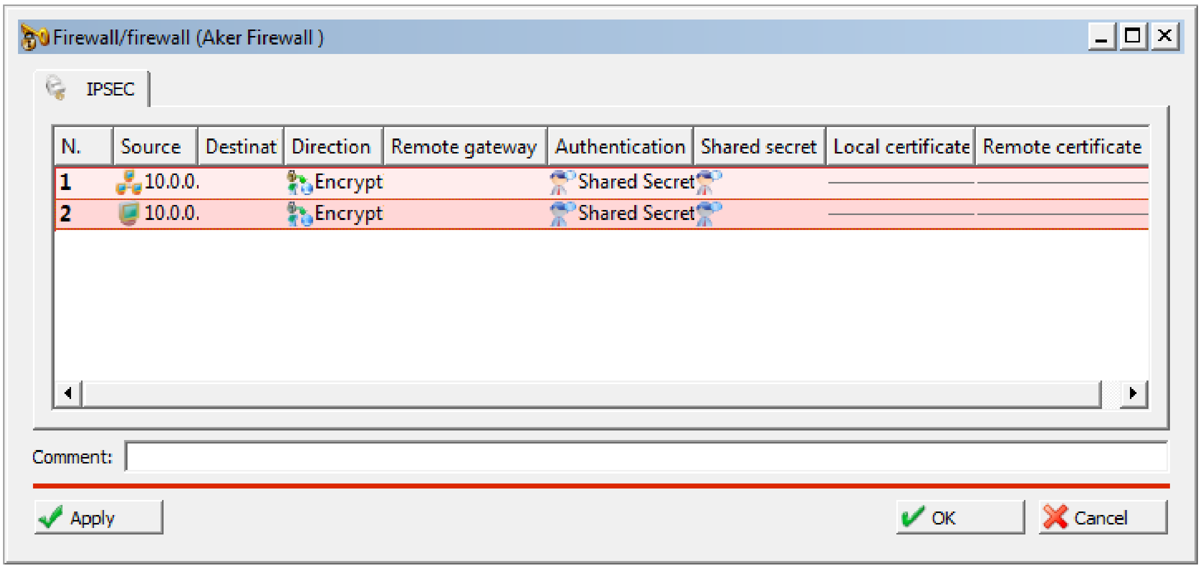

Dispositivos remotos
Firewall - 6.5
Aker Firewall
Aplicação
Auditoria
Configuração do firewall
Configurações do sistema
Criptografia
Certificados IPSEC
Clientes VPN
Firewall/firewall
VPN SSL
Ferramentas
Informação
Segurança
TCP/IP

Figura 232 – Dispositivos remotos (Acesso a janela de Firewall/Firewall).

- Click on the *Cryptography* menu in the main window
- Choose *Firewall-Firewall*

Firewall/firewall



N.	Source	Destinat	Direction	Remote gateway	Authentication	Shared secret	Local certificate	Remote certificate
1	10.0.0.		Encrypt		Shared Secret			
2	10.0.0.		Encrypt		Shared Secret			

Comment:

Image 233 – Firewall/Firewall encryption window.

The cryptography window has the definition of all Aker Firewall encryption flows. Each flow is displayed on a separate line, made out of several cells. Selected flows will be displayed in a different color. The window is composed of four tabs, where each one is used to configure encryption flows using a different key exchange mechanism.

- The **OK** button will update the flow set, which will start operating immediately.
- The **Cancel** button will discard any alteration and close the window.
- The **Apply** button sends all changes to the firewall, and keeps the window open.

- Use the scroll bar on the right side to view flows that do not fit the window.
- Comments associated to selected flows will be displayed on the bottom part of the window.

Hint: A rule position may be modified by drag and dropping it in a new position. Note that the cursor will change into a hand holding a stick.

To execute any operation on a specific flow, just right-click on it and the options below will be displayed (This menu will come up any time the right mouse button is pressed, even if no flow is selected). In this case, only the *Insert* and *Paste* options are enabled.

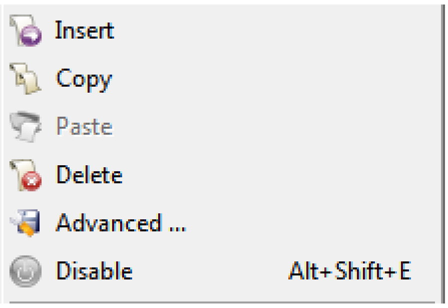


Image 234 – Firewall-firewall options menu.

- **Insert:** adds a new flow to the list. If any flow is selected, the new one will be inserted in its position, pushing it down.
- **Delete:** This option erases the selected flow from the list.
- **Copy:** copies selected flow to a temporary area.
- **Paste:** copies the flow from the temporary area to the list. If a flow on the list is selected, the new one will be copied onto its position, pushing it down. Otherwise, it will be copied to the end of the list.
- **Disable/Enable:** disables or enables the selected flow.

Hint: All these options may be executed from the toolbar in the top part of the window. In this case, first select the flow with the left mouse button, and then click on the desired option in the toolbar.

There are two ways to add or edit flows: drag entities to the desired flow, or right-click over the desired field. In this case, the following options will be available: add, delete, or edit entities, as displayed below:

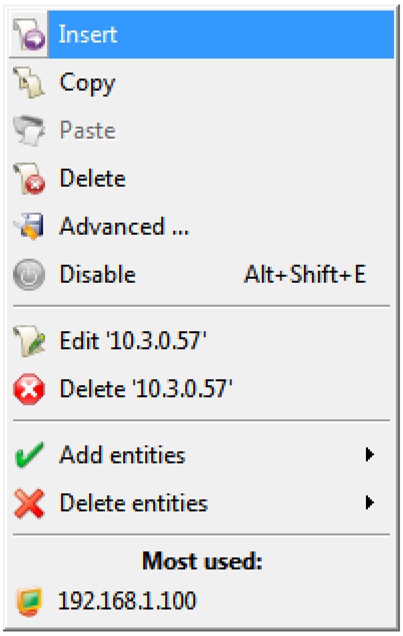
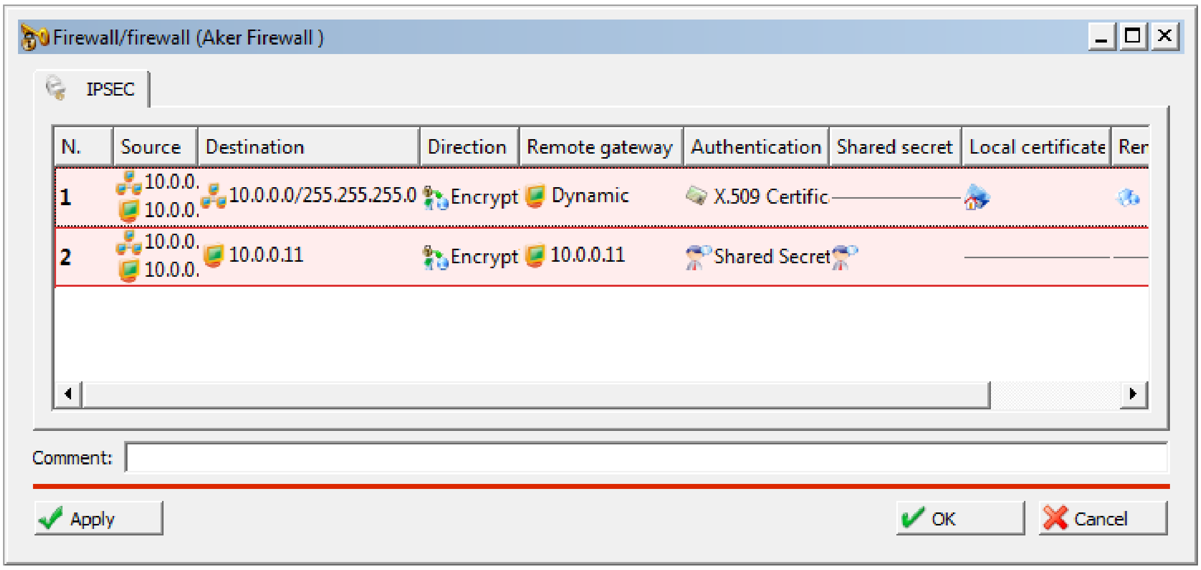

Insert
Copy
Paste
Delete
Advanced ...
Disable Alt+Shift+E
Edit '10.3.0.57'
Delete '10.3.0.57'
Add entities
Delete entities
Most used:
192.168.1.100

Image 235 – Insert menu or flow changes.

Configuring IPSEC tunnels

IPSEC tunnels are used to create a VPN between two networks. The word ‘tunnel’ is applied to differentiate it from common VPNs. Because it effectively creates a virtual channel between involved firewalls, enabling, for example, that networks with invalid addresses communicate securely through the Internet.

To configure IPSEC channels, select the IPSEC tab in the Firewall-Firewall window. This will change the window and display the fields necessary for configuration.


Firewall/firewall (Aker Firewall)
IPSEC

N.	Source	Destination	Direction	Remote gateway	Authentication	Shared secret	Local certificate	Rer
1	10.0.0. 10.0.0.	10.0.0.0/255.255.255.0	Encrypt	Dynamic	X.509 Certific			
2	10.0.0. 10.0.0.	10.0.0.11	Encrypt	10.0.0.11	Shared Secret			

Comment:

Apply
OK
Cancel

Image 236 – IPSEC channels configuration.

Configuration fields meaning:

Source: Defines the entities which addresses will be compared with the *source address* of the *IP packets* that will form the flow.

Destination: Defines the entities which addresses will be compared with the *destination address* of the *IP packets* that will form the flow

Direction: Defines the direction which the flow will be applied. There are only two possible options: the packet that is being encrypted (*encryption*) or the packet which is being decrypted (*decryption*). (For better details, see the topic titled **Planning the Installation)**.

Remote gateway: Defines an entity of type *host* which will become the remote gateway, i.e., in the other side of the IPSEC tunnel is possible defining up to three remote gateways, this way a link redundancy will be created for these tunnels, i.e. in case the first remote gateway link is not operating, a tunnel through the second remote gateway will be established and so on. In the next key exchange will be verified if the first remote gateway is operating and establishing the tunnel.

Now it is possible to add up to 3 remote gateways in the same rule.

Each one of the two firewalls involved in the tunnels need to be sure about the other firewall identity, in order to avoid spoofing attacks (*In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage*). In order of it there are options:

Authentication: Defines the algorithm used in the authentications. The possible values are MD5 or SHA.

Shared secret: A sequence of characters that works as a password and it must to be the same on each side of the tunnel.

Certificate: X.509 certificates are used with a scheme of public Keys for the firewalls identification. This is the same scheme used by secure websites in the Internet.

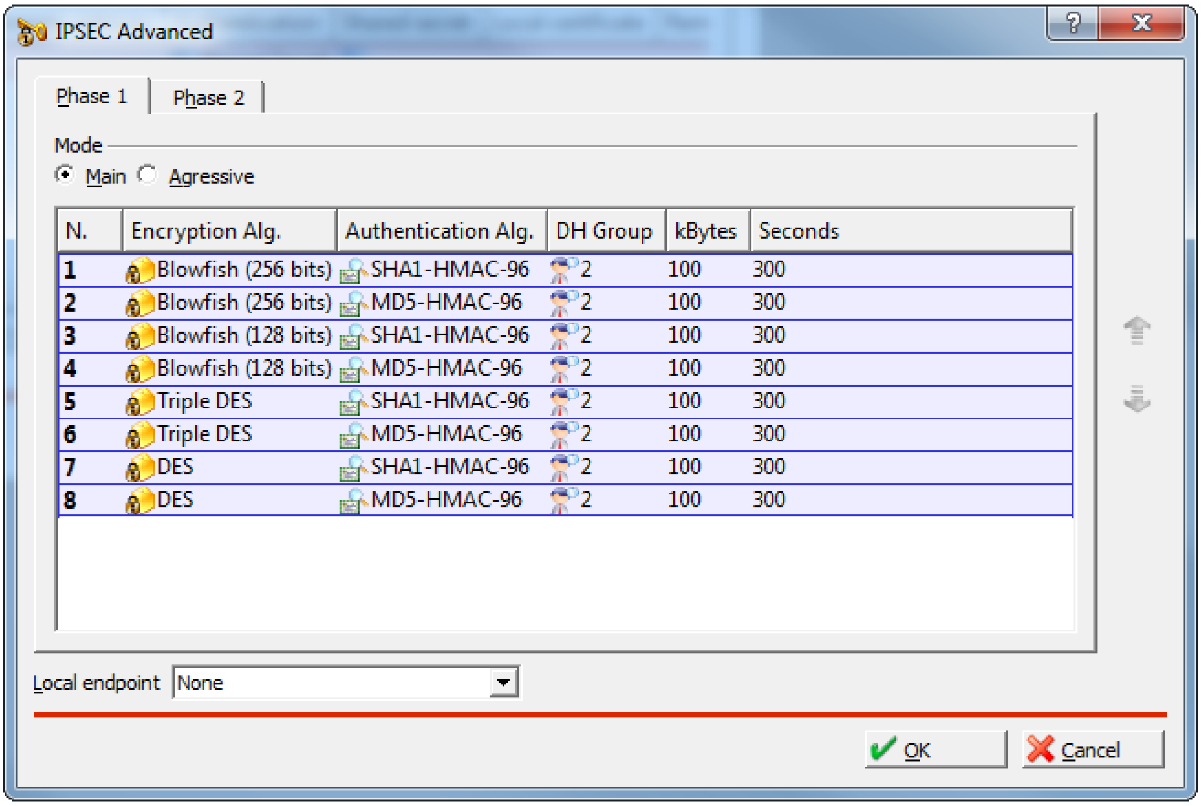
The type shall be specified:

- Local certificate which will be presented to the other side of the tunnel (*Remote Gateway*) and *identification data* required by the *remote firewall*. This data will be an e-mail address for certificates created with the option *USER-FQDN* and a host’s name (*Fully Qualified Domain Dame*), if the option is *FQDN.*

Advanced

The Advanced window is used to set preferred encryption and authentication algorithms and the ones that are allowed by the firewall, during IKE key negotiation. The fields come pre-filled with default algorithms, which may be modified. You will find more information on RFC 2401 and RFC 2412.

The Advanced window, now, includes a choice of the local endpoint, for those cases of invalid intermediary network between the firewall and the router.



Mode
● Main ○ Agressive

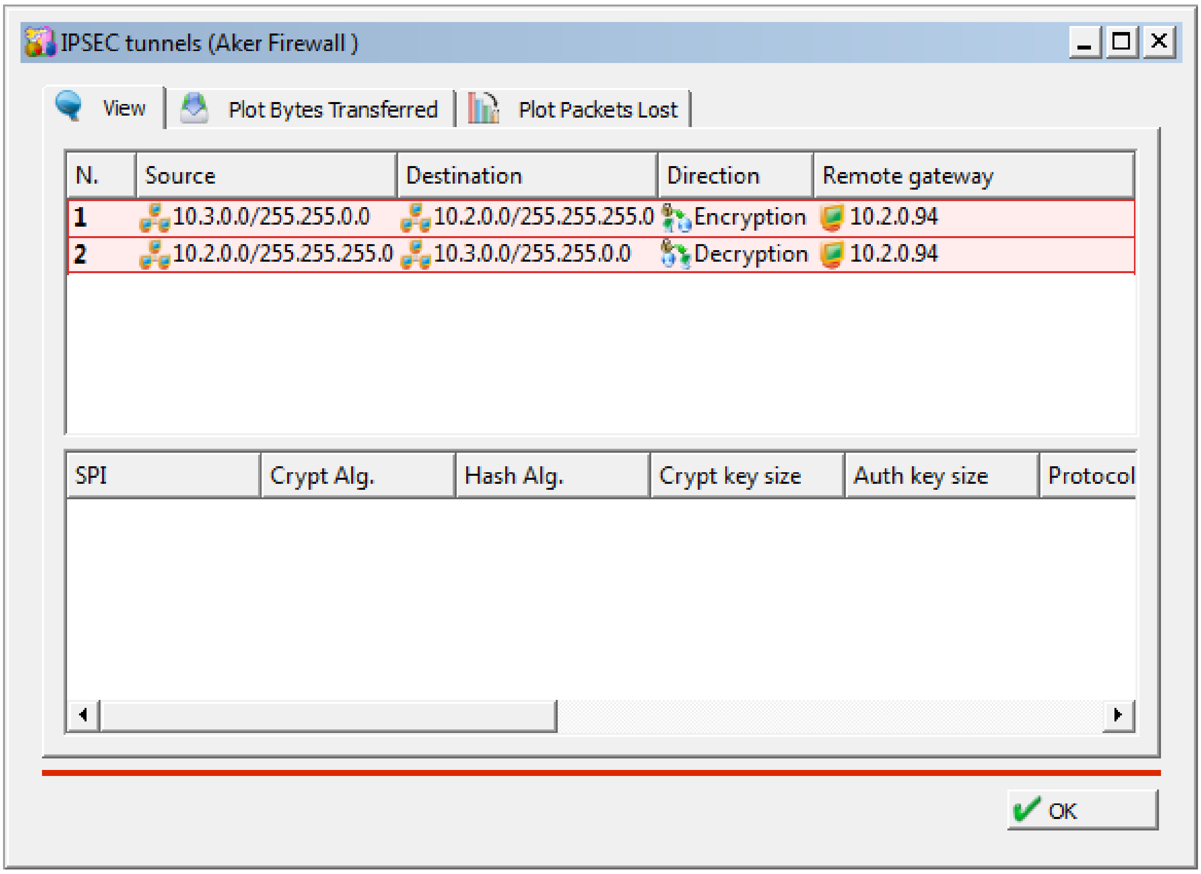
N.	Encryption Alg.	Authentication Alg.	DH Group	kBytes	Seconds
1	Blowfish (256 bits)	SHA1-HMAC-96	2	100	300
2	Blowfish (256 bits)	MD5-HMAC-96	2	100	300
3	Blowfish (128 bits)	SHA1-HMAC-96	2	100	300
4	Blowfish (128 bits)	MD5-HMAC-96	2	100	300
5	Triple DES	SHA1-HMAC-96	2	100	300
6	Triple DES	MD5-HMAC-96	2	100	300
7	DES	SHA1-HMAC-96	2	100	300
8	DES	MD5-HMAC-96	2	100	300

Local endpoint: None

Image 237 – Authentication and encryption algorithm allowed by the firewall during the IKE key trading.

Visualizing the IPSEC traffic

To gain access to the *IPSEC traffic* click on the item *IPSEC Tunnels*, in the *Information menu*.



N.	Source	Destination	Direction	Remote gateway
1	10.3.0.0/255.255.0.0	10.2.0.0/255.255.255.0	Encryption	10.2.0.94
2	10.2.0.0/255.255.255.0	10.3.0.0/255.255.0.0	Decryption	10.2.0.94

SPI	Crypt Alg.	Hash Alg.	Crypt key size	Auth key size	Protocol

Image 238 – Visualizing the IPSEC traffic.

In the window above, is possible to visualize which SPIs IPSEC have been traded to each one of the configured tunnels, simply click on the corresponding rule. If there are more than one SPI, the reason is; the firewall always trades a new SPI before the previous SPI ends, in order to never stop the traffic within the VPN. Above follows the descriptions of each column:

- **SPI:** Security police identification number.
- **Cryptography Algorithm (Crypt Alg):** Show that the cryptography (encryption) algorithm has been traded.
- **Hash Algorithm (Hash alg). :** Shows that the algorithm must to be used to perform the hash of the information.
- **Cryptography Key size (Crypt. key size):** Informs the cryptography key size which both sides of the channel have to use.
- **Authentication key (Auth key size):** Informs the authentication key size.
- **Protocol:** Set of protocols negotiated for the SP.
- **Negotiated bytes:** Amount of bytes that must to be transmitted in order to negotiate a new security policy

- **Transf. bytes:** Amount of bytes transferred by SP.
- **Lost packets:** Packets that have not been decrypted because of some error, so the firewall discards them. In this window the lost packets are accounted.
- **Total Time:** SP expiration date.
- **Idle:** SP downtime.
- **Expiration:** SP expiration date.

When clicking on Plot Bytes Transferred, we can see a graphic of the tunnels which is updated every five seconds. It shows the aggregate traffic of all SPIs of each rule, allowing verifying in real-time the effective use of encrypted bandwidth.

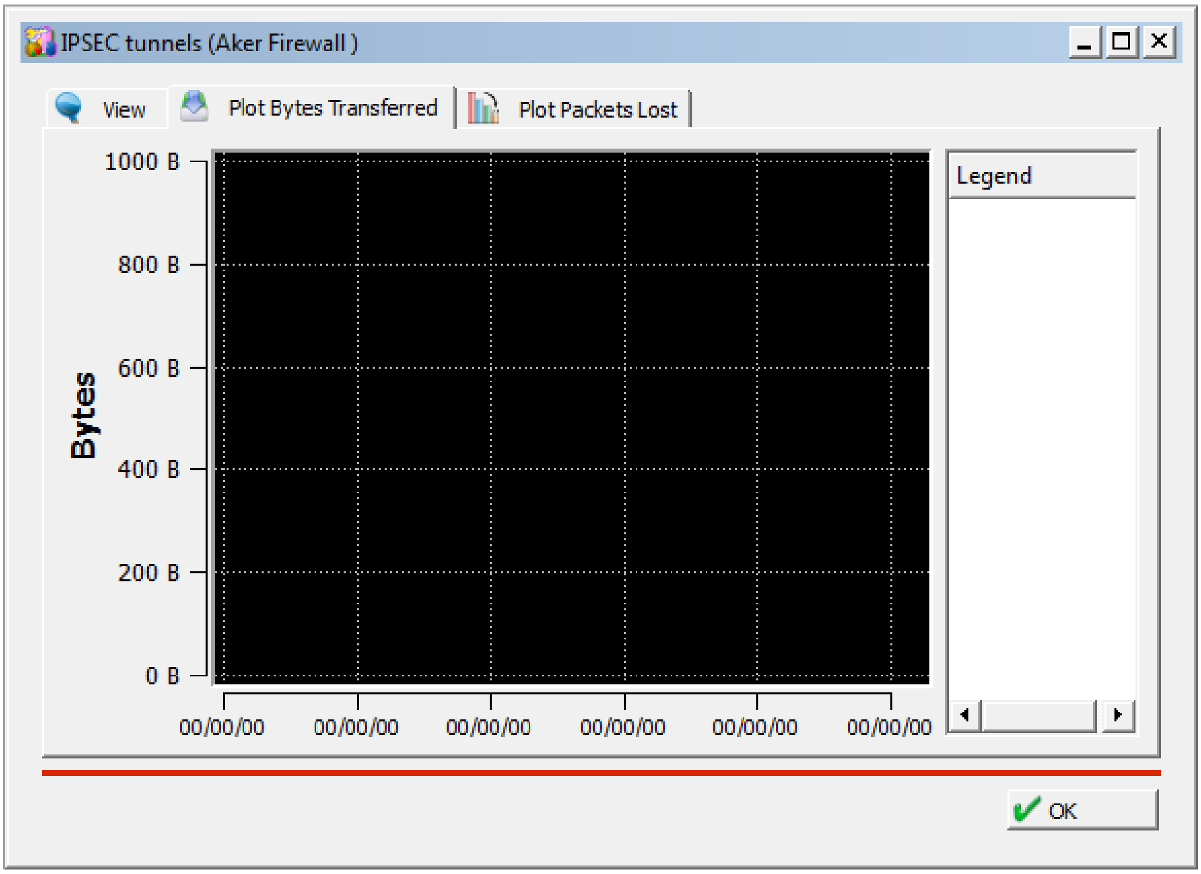

IPSEC tunnels (Aker Firewall)
View
Plot Bytes Transferred
Plot Packets Lost
Bytes
1000 B
800 B
600 B
400 B
200 B
0 B
00/00/00
00/00/00
00/00/00
00/00/00
00/00/00
00/00/00
Legend
OK

Image 239 – Plot of transferred bytes

9.3. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action*).

Loading IPSEC certificates

The command line interface for IPSEC certificate configuration is simple to use, and has the same capabilities as the graphical user interface.

Program Location: */etc/firewall/fwipseccert*

Syntax:

```
   Usage: fwipseccert help
fwipseccert show [request | certificate]
fwipseccert remove [request | certificate] <number>
fwipseccert export <certificate> <file PKCS12> <password>
fwipseccert request <local | remote> <1024 | 2048> <email> <country>
          <state> <city> <organization> <org unit> <domain> [use_email]
          [print]
fwipseccert install <local | remote> <certificate>
fwipseccert import <file PKCS12> <password>
```

Program help:

```
Aker Firewall -
fwipseccert – Requests and X.509 certificates creation and management.
Usage: fwipseccert help
      fwipseccert show [request | certificate]
      fwipseccert remove [request | certificate] <number>
      fwipseccert request <local | remote> <1024 | 2048> <email> <country>
                <state> <city> <organization> <org unit> <domain> [use_email]
                [print]
      fwipseccert install <local | remote> <certificate>
      fwipseccert export <certificate> <file PKCS12> <password>
      fwipseccert import <file PKCS12> <password>

      help      = displays this message
      show       = displays a list of pending requests or installed certificates
      remove     = removes a request or certificate according to its number
      request    = creates a pair of public and private keys along with a x.509
                 certificate request
      install    = installs a x.509 certificate, which pair of keys must have been
                 previously created by the system, through the request command
      export     = exports the certificate and its corresponding pair of keys to a
                 file in the pkcs12 format
      import     = obtains a certificate and its pair of keys, from the pkcs12 file,
                and installs it as the local certificate (see below)

For the request we have:
      local      = the local certificate is used in the firewall’s own identification;
                 it is possible to create several local certificates, however, all
                 of them will use the same pair of keys, generated the first time
                 a local request is generated
      remote     = remotes certificates are used to identify other network entities
      1024/2048 = the two possible key lengths
```

```
use_email = the certificate will have the <email> value as its
          subject alternative name; the <domain> will be the default value
print     = after the request generation, it will be printed on the screen

email, country, state, city, organization, org unit, and domain fields will be
      used to identify the certified user. The field <country> must hold a
      maximum of two digits.  The <org unit> field stands for organization
      unit, and refers to the organization department or division to which
      the certificate user belongs.
```

Loading certificates

The Text Interface of the encryption certificates configuration is simple to use and has the same capacities as the Remote Interface.

Program location: */etc/firewall/fwcert*

Syntax:

```
fwcert help
fwcert show [local | ca | negotiation | revocation]
fwcert load [local | ca] <file> [-f]
fwcert load revocation <file>
fwcert remove <code> [-f]
```

Program help:

```
Aker Firewall
fwcert – Configures the secure channels certificates
Usage: fwcert help
      fwcert show [local | ca | negotiation | revocation]
      fwcert load [local | ca] <file> [-f]
      fwcert load revocation <file>
      fwcert remove <code> [-f]

      help       = shows this message
      show        = shows the specified certificates
      load       = loads a new certificate in the firewall
      remove      = removes a certification authority certificate

For the show command:
      local      = shows the local negotiation certificate
      ca         = shows the certification authority certifications
      negotiation = shows the negotiation certificates of other firewall
                 that has been received through the network
      revocation = shows the revocation certificates that have been loaded
                 locally or received through the network

For the load command:
      local      = loads the local negotiation certificate (if there is a
                 certificate already loaded it will be replaced)
```

ca = loads a certification authority certificate which will be used to validate the received negotiation certificates
revocation = loads a revocation certificate which will be used to invalidate a compromised negotiation certificate
file = file name which the certificate will be loaded from
-f = if present, will cause the program not to confirm when replacing a certificate

For the remove command:
code = code of the certification authority to be removed
-f = if presented, will cause the program not to confirm when removing a certificate

Example 1: (loading the local certificate)

```
#/etc/firewall/fwcert load local /tmp/firewall.crt
Loading certificate...OK
```

Example 2: (viewing the certification authorities certificates)

```
#/etc/firewall/fwcert show ca
Name: Aker Security Solutions
Code: 1

Name: Authorized Certification Authority
Code: 2
```

Example 3: (loading a new certification authority certificate)

```
#/etc/firewall/fwcert load ca /tmp/new_ca.ca
Certificate added
```

Example 4: (removing a certification authority certificate, without confirmation)

```
#/etc/firewall/fwcert remove 2 -f
Certification authority removed
```

Configuring Firewall-Firewall channels

The use of the Text Interface in the configuration of the secure channels creates a difficulty caused by the great number of arguments that should be passed through the command line.

This Text Interface has the same capacities of the Remote Interface except that it is not possible to assign comments for secure channels, specify more than one entity to the source or destination of the secure channels, nor specify algorithms to Aker-CDP key exchange through this interface (when using Aker-CDP, all algorithms will always be set to automatic). It will neither be possible to configure algorithms to be used by IPSEC-IKE (Advanced window); they will always have default values.

***Program location**: /etc/firewall/fwcripto*

***Syntax**:*

```
fwcripto [show | help]
fwcripto [enable | disable | remove]  <pos>

fwcripto add <pos> <source> <destination> <send | receive>
        ipsec <gateway> <<ss <secret> | cert <local> <remote>>
fwcripto add <pos> <source> <destination> <send | receive>
        manual <spi> [MD5 | SHA] <authentication key> NONE
fwcripto add <pos> <source> <destination> <send | receive>
        manual <spi> [MD5 | SHA] <authentication key>
        [DES | BFISH128 | BFISH256] <iv size> <encryption key>
fwcripto add <pos> <source> <destination> <send | receive>
        manual <spi> [MD5 | SHA] <authentication key>
        3DES <iv size> <key1> <key2> <key3>
fwcripto add <pos> <source> <destination> send
        skip [DES | 3DES | BFISH256] [MD5 | SHA]
        [NONE | DES | 3DES | BFISH128 | BFISH256] <secret>
fwcripto add <pos> <source> <destination> receive
        skip <secret>
fwcripto add <pos> <source> <destination> <send | receive> aker-cdp
```

Program help:

```
Aker Firewall
fwcripto – Configures the secure channels table
Usage: fwcripto [show | help]
      fwcripto remove <pos>
      fwcripto add <pos> <source> <destination> <send | receive>
              ipsec <gateway> <<ss <secret> | cert <local> <remote>>
      fwcripto add <pos> <source> <destination> <send | receive>
              manual <spi> [MD5 | SHA] <authentication key> NONE
      fwcripto add <pos> <source> <destination> <send | receive>
              manual <spi> [MD5 | SHA] <authentication key>
              [DES | BFISH128 | BFISH256] <iv size> <encryption key>
      fwcripto add <pos> <source> <destination> <send | receive>
              manual <spi> [MD5 | SHA] <authentication key>
              3DES <iv size> <key1> <key2> <key3>
      fwcripto add <pos> <source> <destination> send
              skip [DES | 3DES | BFISH256] [MD5 | SHA]
              [NONE | DES | 3DES | BFISH128 | BFISH256] <secret>
      fwcripto add <pos> <source> <destination> receive
              skip <secret>
      fwcripto add <pos> <source> <destination> <send | receive> aker-cdp

      show     = shows all entries in the secure channels table
      add      = adds a new entry to the table
      remove   = removes an existing entry from the table
      help      = shows this message

To add:
      pos       = position where the new entry will be added
                (It can be a positive integer or the word END, to add the
                 new entry at the end of the table)
      send       = this entry will be used when sending packets
      receive   = this entry will be used when receiving packets
      ipsec     = uses IPSEC key exchange protocol
      gateway   = the entity representing the remote end of the IPSEC tunnel
      ss        = uses Shared Secret for authentication
      secret    = the string to be used as the shared secret
      cert      = uses X.509 certificates for authentication
      local     = the domain name in the local certificate to present
      remote    = the domain name in the remote certificate to expect
      manual    = uses manual key exchange
      skip      = uses SKIP for automatic key exchange
      aker-cdp = uses Aker-CDP for automatic key exchange
      spi       = Security Parameter Index
                (It is an integer that identifies the security association
                 between the source and destination hosts. This number must
                 be greater than 255)
      MD5       = uses the MD5 as the authentication algorithm
      SHA       = uses the SHA-1 as the authentication algorithm
      DES       = uses the DES as the encryption algorithm
      3DES      = uses the triple DES as the encryption algorithm
      BFISH128 = uses the Blowfish with 128 bits keys as the encryption
                algorithm
      BFISH256 = uses the Blowfish with 256 bits keys as the encryption
                algorithm
      NONE      = does not use encryption, only authentication
                (for the skip, the first selected algorithm corresponds
                 to the key encryption algorithm and the second one to the
                 packet encryption)
      iv_size   = initialization vector size, in bits, for the encryption
                algorithm. It value must be either 32 or 64.

      The authentication key, encryption key(s) and the skip secret
      must be typed as hexadecimal digits.
      For the 3DES, 3 keys separated by spaces must be typed

To remove:
      pos       = position to be removed from the table
                (the position is the value displayed on the left of each entry
                 when the show command is invoked)
```

Redundancy of a private link with a site-to-site VPN

The command fwlinkred allows the link load balancing that uses a point-to-point dedicated link and a VPN, to keep a connection secure between two points, even if the dedicated link goes offline.
This Text Interface has the same capacities of the Remote Interface except that it is not possible to assign comments for secure channels.

Program location:/aker/bin/firewall/fwlinkred

Syntax:

```
/aker/bin/firewall # fwlinkred help

Aker Firewall

Usage: fwlinkred help

    fwlinkred show

    fwlinkred add <link> <vpn1> [vpn2] ... [vpnN]

    fwlinkred remove < rule >

    fwlinkred < enable | disable > < rule >

Where:

    <link> load balancing rule name

    <vpnN>  VPN IPSEC rule number

    <rule>  redundancy rule number
```

Configuring Client-Firewall secure channels

10. Configuring Client-Firewall secure channels

This chapter shows how to configure the firewall and the Aker Client in order to provide the creation of secure channels between client hosts and an Aker Firewall.

10.1. Planning installation

What is a Client-Firewall secure channel?

As detailed in the previous chapter, a secure client-firewall channel is established directly between a client host and an Aker Firewall. This is possible through the installation of Aker Encryption Client in client hosts.

A Client-Firewall encryption channel uses the same encryption, authentication, and key exchange technologies as secure firewall-firewall channels do, with the difference that everything is automatically negotiated by the communicating entities. Manually, the administrator can only disable certain algorithms, to ensure they will not be used.

Another difference between secure firewall-firewall and client-firewall channels regards their implementation in the Firewall Aker. While firewall-firewall is always done in IP packets level, where each packet is individually encrypted, with client-firewall it is done in the data flow level, where only the information the packet is carrying is encrypted (and not other IP packet data).

Requirements for creating Client-Firewall secure channels

To establish secure channels between clients and a firewall, the following conditions must be met:

1. Aker Client should be installed in every computer which will establish secure channels with the firewall, in case they use the Secure Roaming;

or

2. Client support for L2TP or PPTP protocol.

Defining a client-firewall secure channel

A client-firewall secure channel configuration is much simpler than that of a firewall-firewall channel. It is only necessary to define, in the firewall, which hosts will establish client secure channels, and whether user authentication will be performed. All other procedures are done automatically, when the client initiates the secure channel negotiation.

10.2. Aker Secure Roaming

To gain access to the Secure Roaming configuration window, follow the steps bellow:

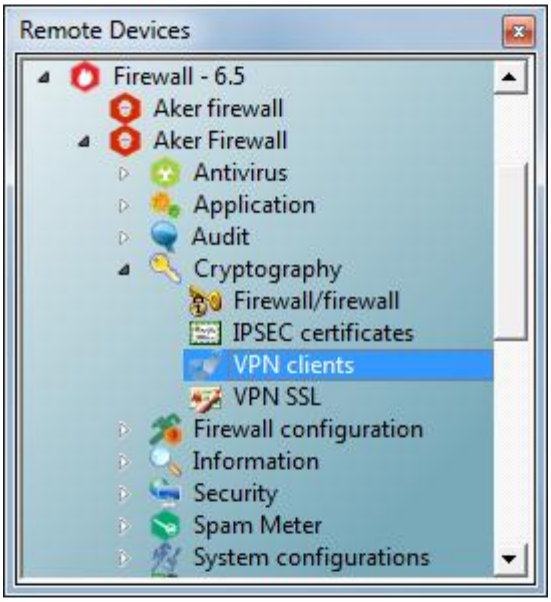
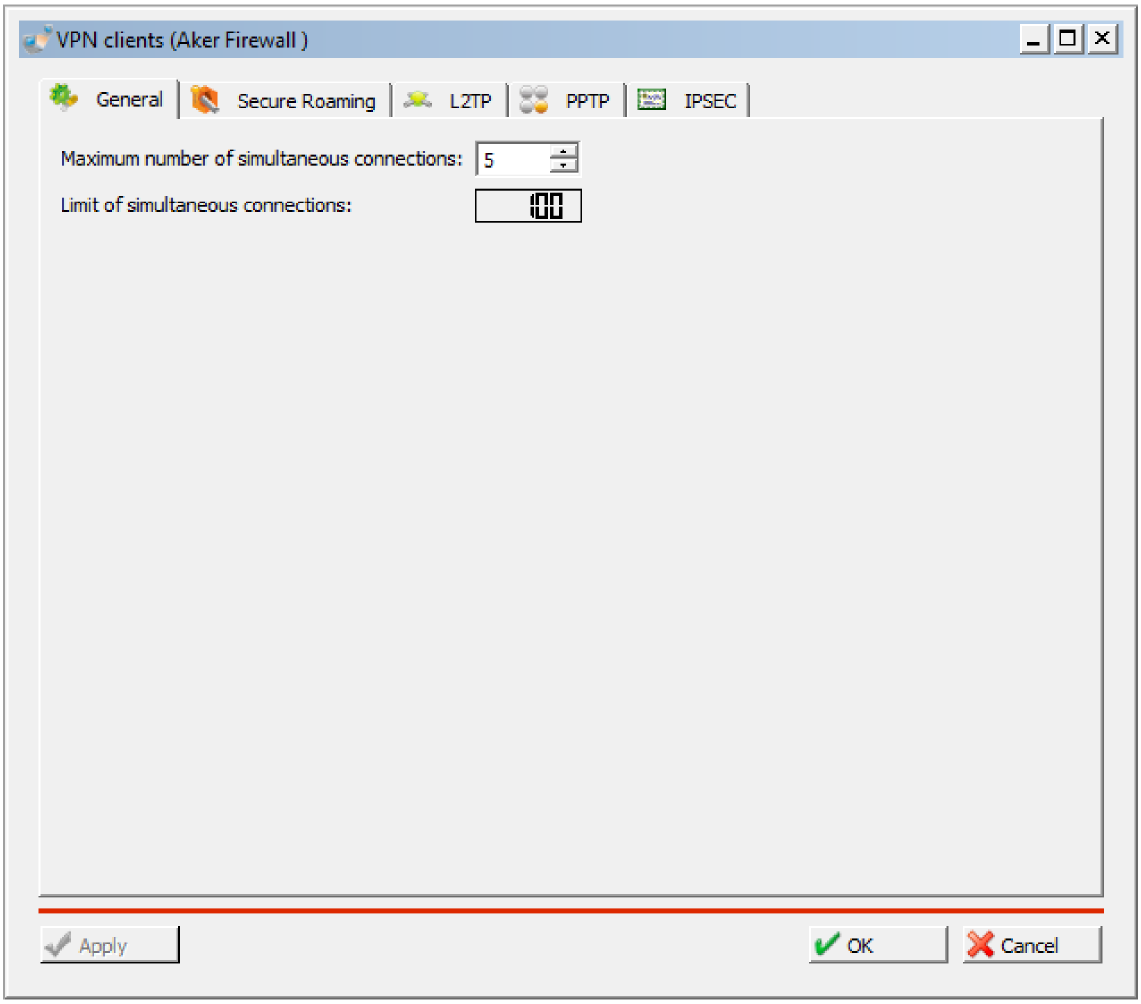

Remote Devices
Firewall - 6.5
Aker firewall
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall/firewall
IPSEC certificates
VPN clients
VPN SSL
Firewall configuration
Information
Security
Spam Meter
System configurations

Image 240 – Remote devices (Gaining access to the *Secure Roaming configuration*).

- Click on the Cryptography menu in the main window;
- Choose *VPN clients*.

Secure Roaming configuration window



Maximum number of simultaneous connections: 5

Limit of simultaneous connections: 100

Image 241 – Security Roaming standard configuration.

- The **OK** button closes the Secure Roaming window and saves the changes applied by the user;
- The **Cancel** closes the Secure Roaming window but does not apply the changes made by the user ;
- The **Apply** button will save all changes to the firewall but the window will remain opened;

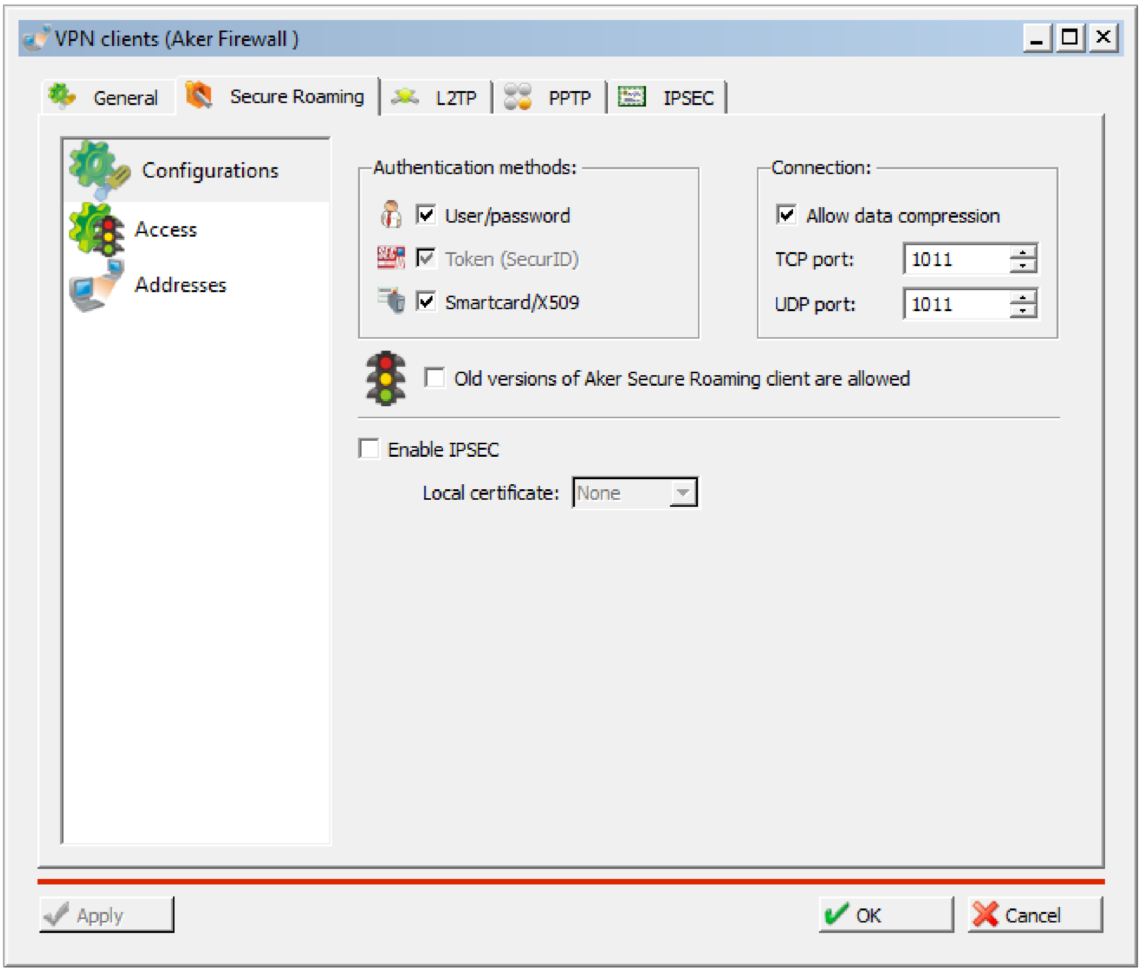
General tab

- **Maximum number of simultaneous connections**: Here you can configure the maximum number of clients connected simultaneously in the Secure Roaming, L2TP or PPTP. Use this option to avoid the server of getting overload by too many clients that can decrease the performance.

The number cannot be larger than its license. If the number is 0, no client will be allowed.

- **Limit of simultaneous connections**: Indicate the maximum limit of simultaneous connections for your license.

Secure Roaming tab



Authentication methods:
☑ User/password
☑ Token (SecurID)
☑ Smartcard/X509

Connection:
☑ Allow data compression
TCP port: 1011
UDP port: 1011

☐ Old versions of Aker Secure Roaming client are allowed

☐ Enable IPSEC
Local certificate: None

Image 242 – Security Roaming Configuration

- **Authentication methods**: The available options are:

1. **User/password:** The user shall be authenticated through a combination of name and password. These data will be passed on to one or more authentication server that shall authenticate user and password;
2. **Token (SecurID):** The user shall be authenticated through a name, a PIN or a code present in a Token SecurID which is modified every minute. These data will be passed on to the Token authenticator registered in the firewall to be validated. This option is more secure than the previous one, but requires from all users a Token;
3. **Smartcard/X.509:** The user shall be authenticated through x.509 certificates (e.g. written in a smart card). This options is the most secure of the three

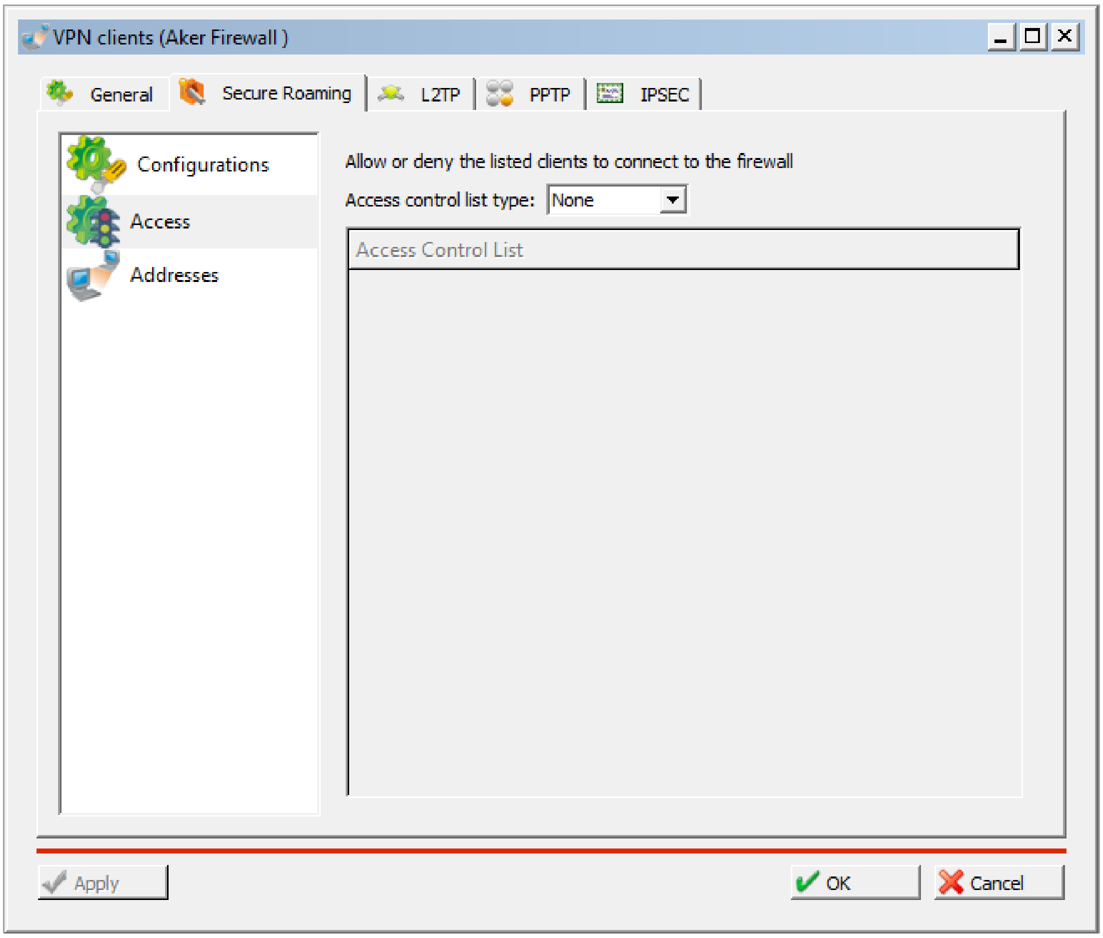
authentication methods because requires from each user a password to unlock the private key ;

- **Old versions of Aker Secure Roaming client are allowed:** Allows connection of old versions of Aker Secure Roaming Client.

- **Enable IPSEC**: Uses IPSEC protocol in the connection with Secure Roaming.

- **Allow data compression**: The data compression is important for slow connections such as dial-up. When this option is checked, it will compress the information before it be sent by the network. This allows a gain in the performance of communication speed, but requires a greater local processing. For faster networks, it is not recommended to use compression.
- **TCP/UDP port**: This control allows configuring the port used by server to listen the clients' data and connections. For instance, you can configure the server to use the TCP/443 ports and UDP/52 in order to swindle firewalls or other filtering devices between servers and clients. These devices would refuse a VPN connection, but would not refuse a secure HTTP connection and a DNS request. Standard port is **1011** for both TCP and UDP.

Access subtab



Allow or deny the listed clients to connect to the firewall

Access control list type: None

Access Control List

Image 243 – Security Roaming access control list.

- **Access control list type**: Here you choose which is the access control list type

1. **None**: Without access control. All clients have permission to connect to the server.
2. **Allow listed**: Only listed IP addresses, or addresses belonging to network entities or set listed, will be allowed to establish connection.
3. **Denied listed**: The listed IP addresses, or addresses belonging to network entities or set listed, will not be allowed to establish connection:

Access Control List:

To add an entity in the list, follow the steps bellow:

- Right-click on the list;
  or
- Drag the entity form the entity field (F5) to the access control list, and drop it there;

To remove an entity, follow the steps bellow:

- Right-click on the selected entity, and click on the option *Delete Entities*
  or
- Select the entity you wish to delete and press the *Delete key* on your keyboard.

The following Image shows the pop-up menu with all options listed above. You can have access it right-clicking on any listed entity:

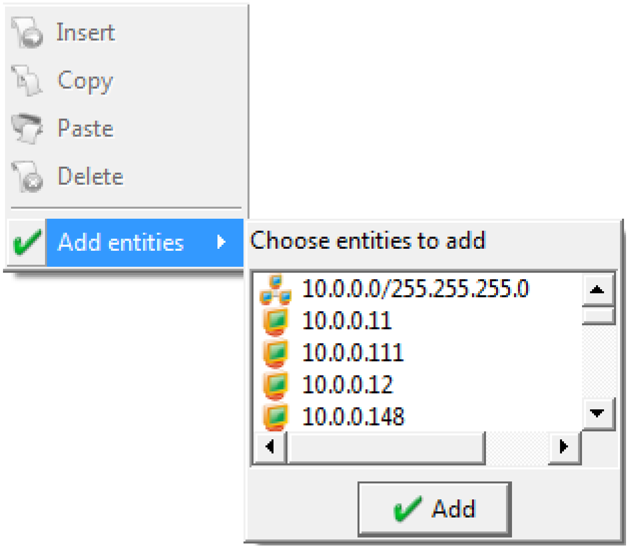
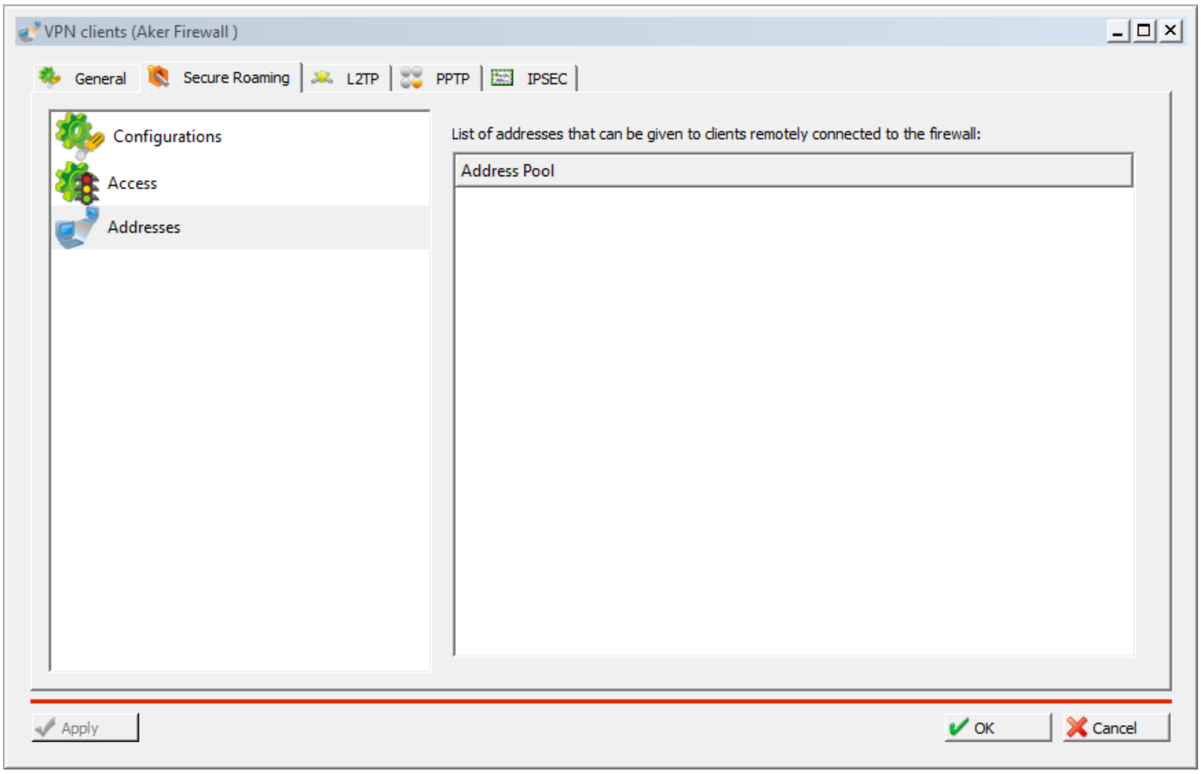

Insert
Copy
Paste
Delete
Add entities
Choose entities to add
10.0.0.0/255.255.255.0
10.0.0.11
10.0.0.111
10.0.0.12
10.0.0.148
Add

Image 244 – Pop-up menu.

Addresses subtab


VPN clients (Aker Firewall)
General
Secure Roaming
L2TP
PPTP
IPSEC
Configurations
Access
Addresses
Address Pool
Apply
OK
Cancel

List of addresses that can be given to clients remotely connected to the firewall:

Image 245 – Security Roaming address pool.

- **Address Pool**: List of addresses that can be assigned to clients connected remotely to the firewall. The addresses installed hosts, all addresses that compose the network, and the included pool, together, they add up in order to define the address Pool attributable to clients. Take note that the listed entities must to be connected to any network adapter in the firewall. Otherwise, will not be possible establishing connection with such entity.

The networks in this field define an address pool, not a subnetwork in sense of *IP routing*. It means, if the firewall's interface is located at subnetwork 10.0.0.0/255.0.0.0 and the network 10.0.0.0/255.255.255.0 is included in the address pool, the first attributable address would be 10.0.0.1 and the last 10.0.0.255. If it were the network 10.1.0.0/255.255.255.0, the range would go from 10.1.0.0 to 10.1.0.255, adding itself in both sides.

10.3. L2TP

In computer networking, *Layer 2 Tunneling Protocol (L2TP)* is a tunneling protocol used to support virtual private networks *(VPNs)* or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

Published in *1999* as proposed *standard RFC 2661, L2TP* has its origins primarily in two older tunneling protocols for Point-to-Point Protocol (PPP): *Cisco's Layer 2 Forwarding Protocol (L2F)* and *USRobotics Point-to-Point Tunneling Protocol (PPTP)*. A new version of this protocol, *L2TPv3*, was published as proposed *standard RFC 3931 in 2005*. *L2TPv3* provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (e.g., Frame Relay, Ethernet, ATM, etc.).

The entire *L2TP packet*, including payload and *L2TP header*, is sent within a User Datagram Protocol UDP datagram. It is common to carry *Point-to-Point Protocol (PPP)* sessions within an *L2TP* tunnel. *L2TP* does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as *L2TP/IPsec* (discussed below).

The two endpoints of an *L2TP* tunnel are called the *LAC (L2TP Access Concentrator)* and the *LNS (L2TP Network Server)*. The LAC is the initiator of the tunnel while the *LNS* is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP *session* (or 'call') is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorized as either *control packets* or *data packets*. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

Layer 2 Tunneling Protocol Version 3 is an IETF standard related to L2TP that can be used as an alternative protocol to *Multiprotocol Label Switching (MPLS)* for encapsulation of multiprotocol Layer 2 communications traffic over IP networks. Like *L2TP, L2TPv3* provides a ‘pseudo-wire’ service, but scaled to fit carrier requirements.

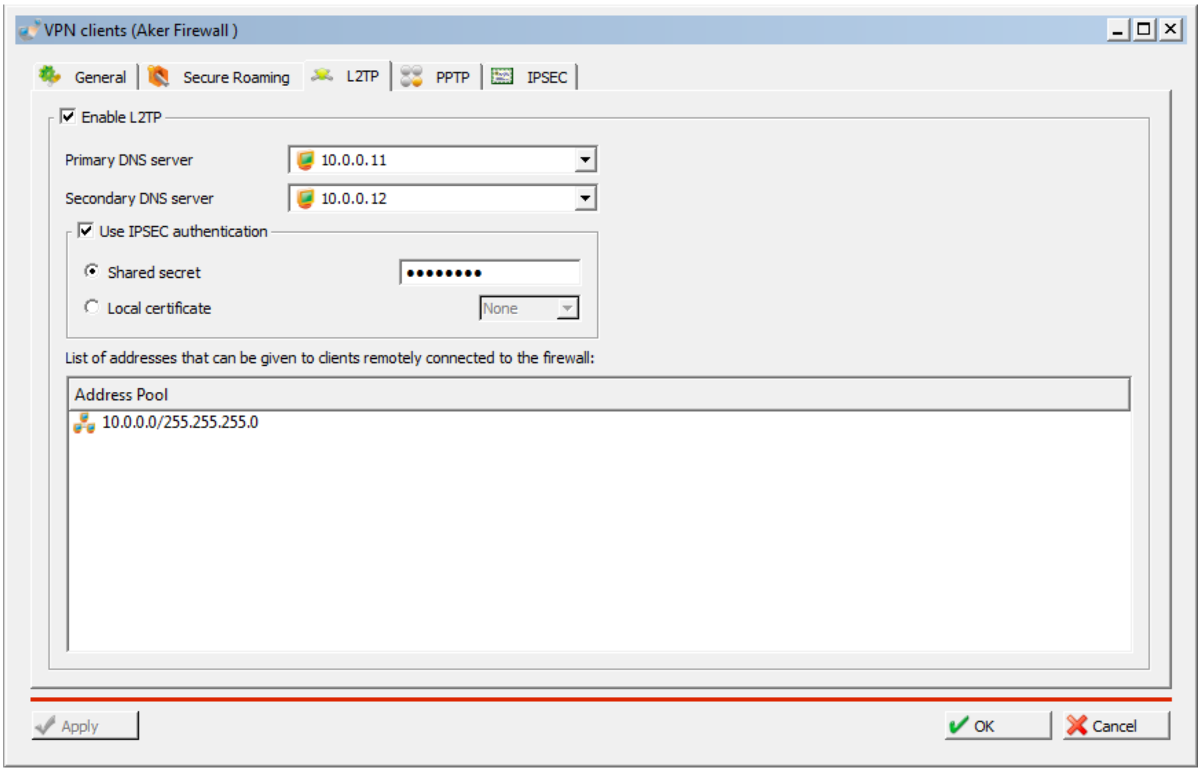
L2TPv3 can be regarded as being to *MPLS* what IP is to ATM: a simplified version of the same concept, with much of the goodness achieved with a fraction of the effort, at the cost of losing some technical features considered less important in the market. In the case of *L2TPv3,* the features lost are *teletraffic* engineering features considered important in MPLS. The *protocol overhead* of L2TPv3 is also significantly bigger than *MPLS*. However, there is no reason why these features could not be re-engineered in or on top of *L2TPv3* in later products

L2TP advantages:

- Users can take advantage of the low cost of the Internet. Instead of making a long-distance call to connect;
- Easy configuration for the client;
- directly with the corporate website's remote access server, remote users dial in to a local ISP and use the Internet;
- To handle all long-distance connections;

- The protocol provides virtual dial-up because the user does not really dial in to the corporate network, but when the connection is complete, it is as if he does. This enables outsourcing of dial-up services to the ISP and support of roaming users;
- Because PPP framing is used, remote users can access corporate sites using a variety of protocols such as IP, IPX, SNA, and so on;
- The corporate site assigns an IP address to a remote client instead of the ISP. This alleviates the address shortage problem with ISPs and the Internet;
- L2TP provides end-system transparency, meaning that the remote user does not require any special software to use the service in a secure way;
- An organization can control the authentication of users instead of the ISP;

Configuring the VPN L2TP



VPN clients (Aker Firewall)
General
Secure Roaming
L2TP
PPTP
IPSEC
Apply
OK
Cancel

☑ Enable L2TP

Primary DNS server: 10.0.0.11

Secondary DNS server: 10.0.0.12

☑ Use IPSEC authentication

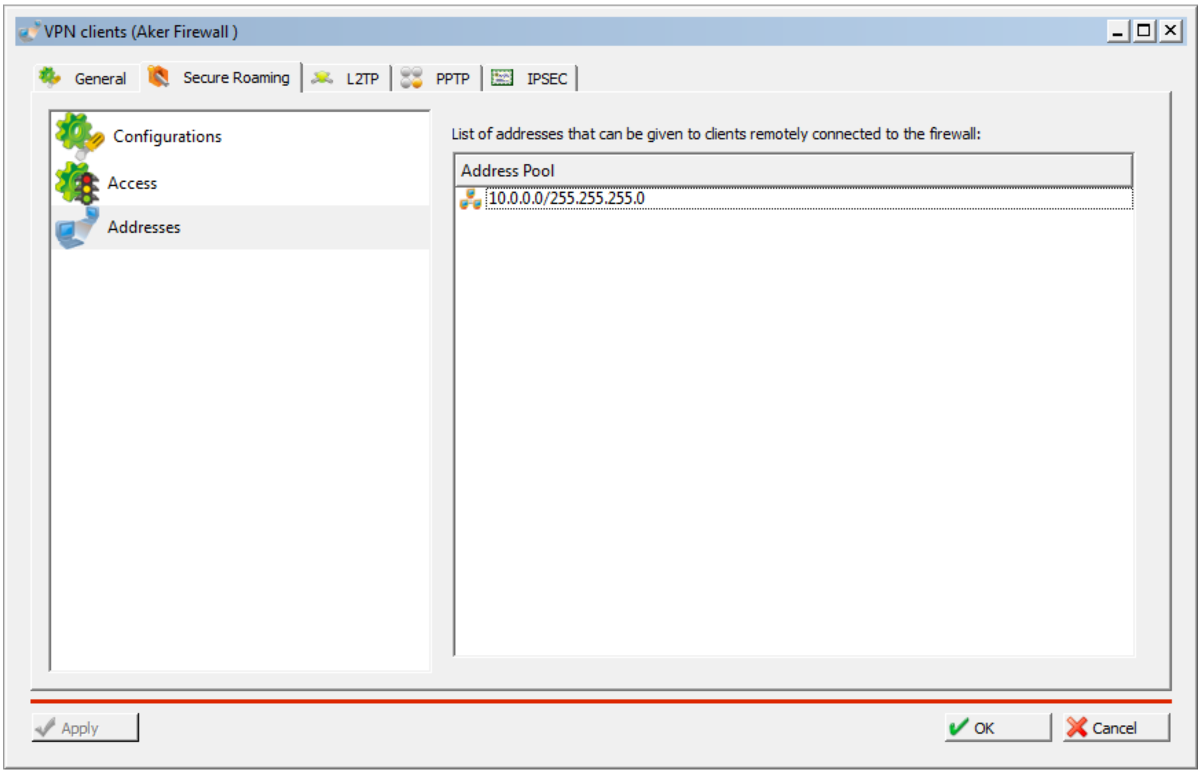
● Shared secret: ●●●●●●●●●

○ Local certificate: None

List of addresses that can be given to clients remotely connected to the firewall:

Address Pool
10.0.0.0/255.255.255.0

Image 246 – L2TP configuration.



List of addresses that can be given to clients remotely connected to the firewall:

Address Pool
10.0.0.0/255.255.255.0

Image 247 – List of addresses that can be provided to clients connected remotely to the firewall.

- **Enable L2TP:** This field enables the L2TP server in Aker Firewall and allows configuring other fields such as:
    - **Primary and Secondary DNS servers:** Configure two DNS servers to be used during the encrypted session;
    - **Use IPSEC authentication:** Enable the authentications modes and L2TP data encapsulation in IPSEC packets, the authentication modes are done through the “Shared secret or x.509 certificate”

- **Address Pool:** List of addresses that can be assigned to clients connected remotely to the firewall. The addresses installed hosts, all addresses that compose the network, and the included pool, together, they add up in order to define the address Pool attributable to clients. Take note that the listed entities must to be connected to any network adapter in the firewall. Otherwise, will not be possible establishing connection with such entity.

  To add an entity to the list, follow the steps bellow:

    - Right-click on the list and select *Add entities*,
      or
    - Drag the entity form the entity field (F5) to the access control list, and drop it there;

  To remove an entity, follow the steps bellow:

    - Right-click on the selected entity, and click on the option *Delete Entities* or

- Select the entity you wish to delete and press the *Delete key* on your keyboard.

The following Image shows the pop-up menu with all options listed above. You can have access it right-clicking on any listed entity:

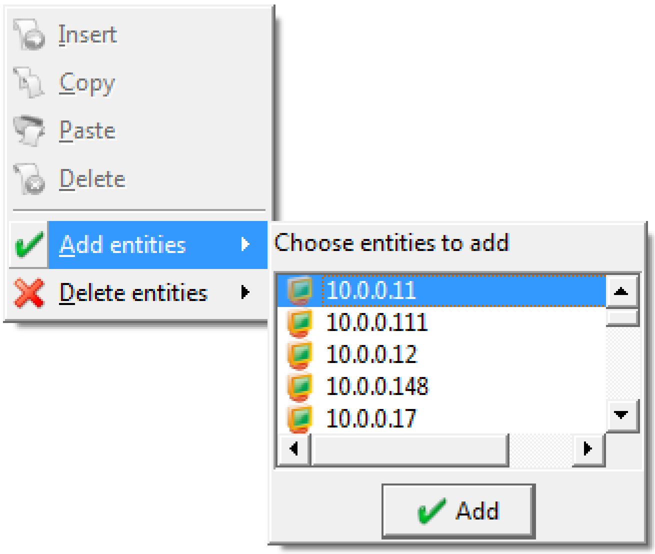

Insert
Copy
Paste
Delete
Add entities
Delete entities
Choose entities to add
10.0.0.11
10.0.0.111
10.0.0.12
10.0.0.148
10.0.0.17
Add

Image 248 – Pop-up menu.

The networks in this field define an address pool, not a subnetwork in sense of *IP routing*. It means, if the firewall’s interface is located at subnetwork 10.0.0.0/255.0.0.0 and the network 10.0.0.0/255.255.255.0 is included in the address pool, the first attributable address would be 10.0.0.1 and the last 10.0.0.255. If it were the network 10.1.0.0/255.255.255.0, the range would go from 10.1.0.0 to 10.1.0.255, adding itself in both sides.

Using the text Interface

```
# fwl2tp help

Firewall Aker – Version 6.5
Use: fwl2tp help

fwl2tp show
fwl2tp < enable | disable >
fwl2tp clean
fwl2tp ipsec ss < secret >
fwl2tp ipsec cert < fqdn >
fwl2tp ipsec none
fwl2tp dns_1 < dns_server >
fwl2tp dns_2 < dns_server >
fwl2tp add < network >
```

fwl2tp delete < network>

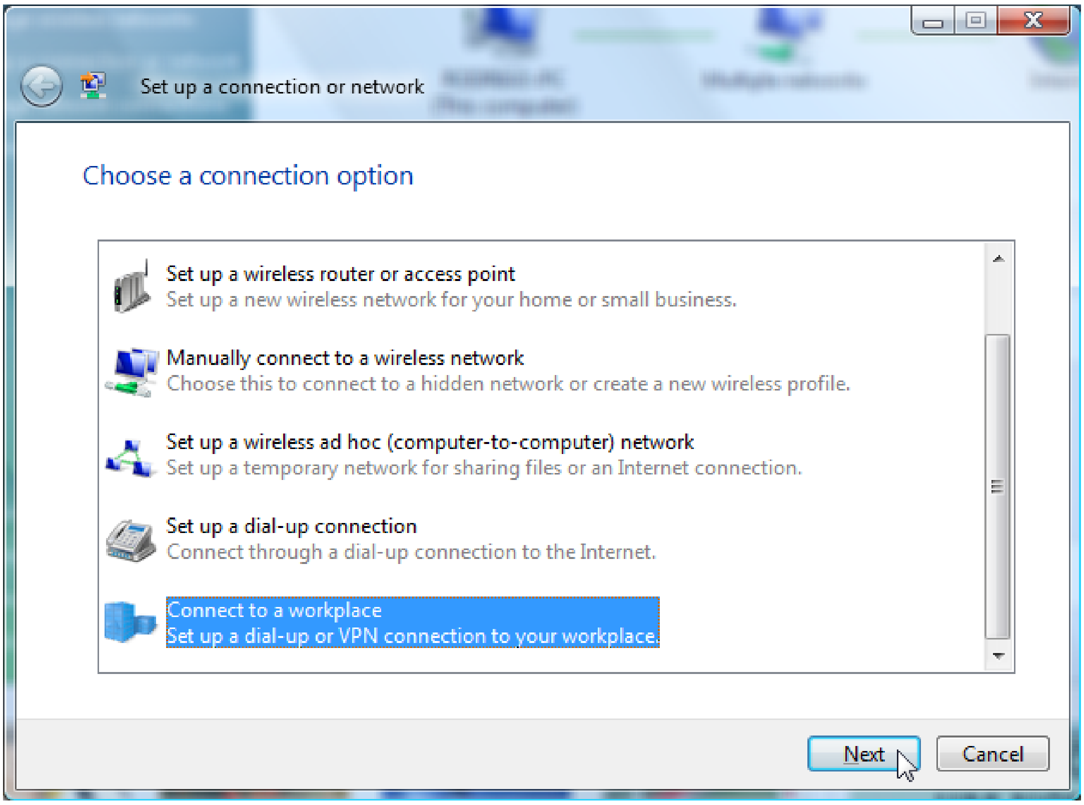
The parameters are:

secret: The IPSEC shared secret
fqdn: Domain name present in the X.509 certificate for IPSEC authentication
dns_server: A DNS server (entity) for VPN clients
network: host or network entity for the VPN Clients' IP address pool

Configuring the L2TP client

Windows 7 / XP

On *Windows 7*, you need to create a new VPN connection on *Network and Sharing Center*. On *Windows XP*, it shall be done at the window *Network Connections. A wizard* to assist you in the creation of this connection will be displayed, and must be filled in as described in the Images bellow:



Set up a connection or network

Choose a connection option

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

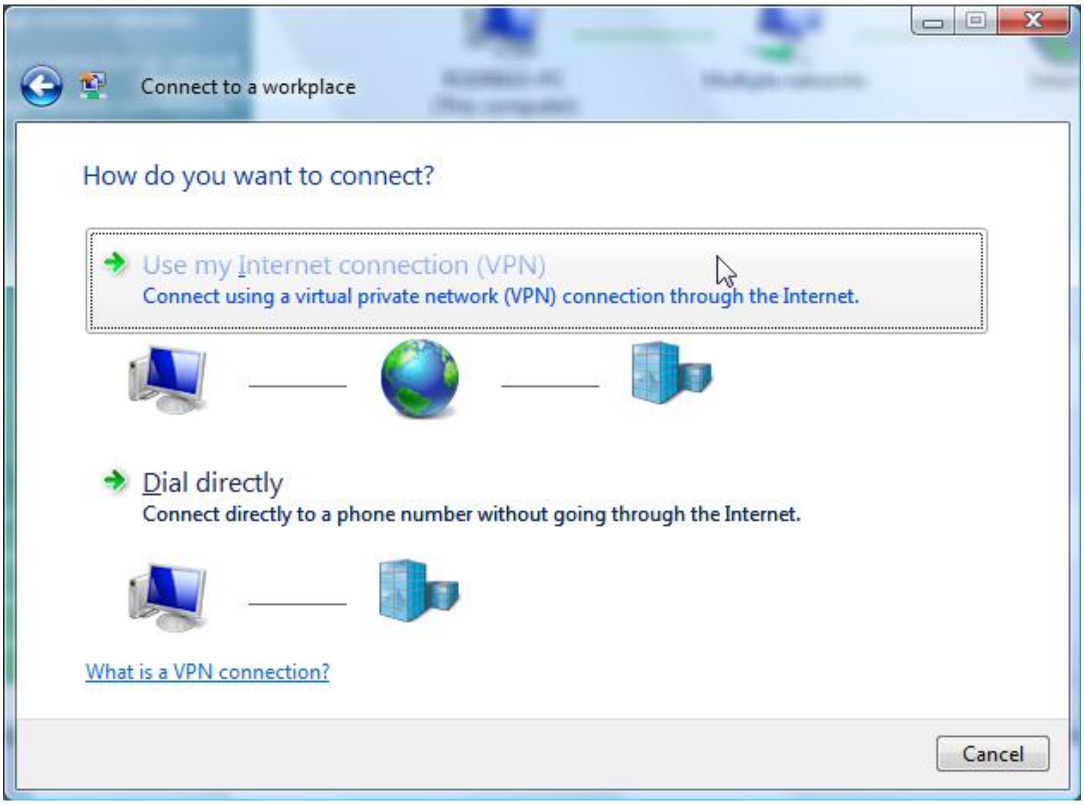
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.

Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Image 249 – Configuring the L2TP client (Windows Vista/XP).



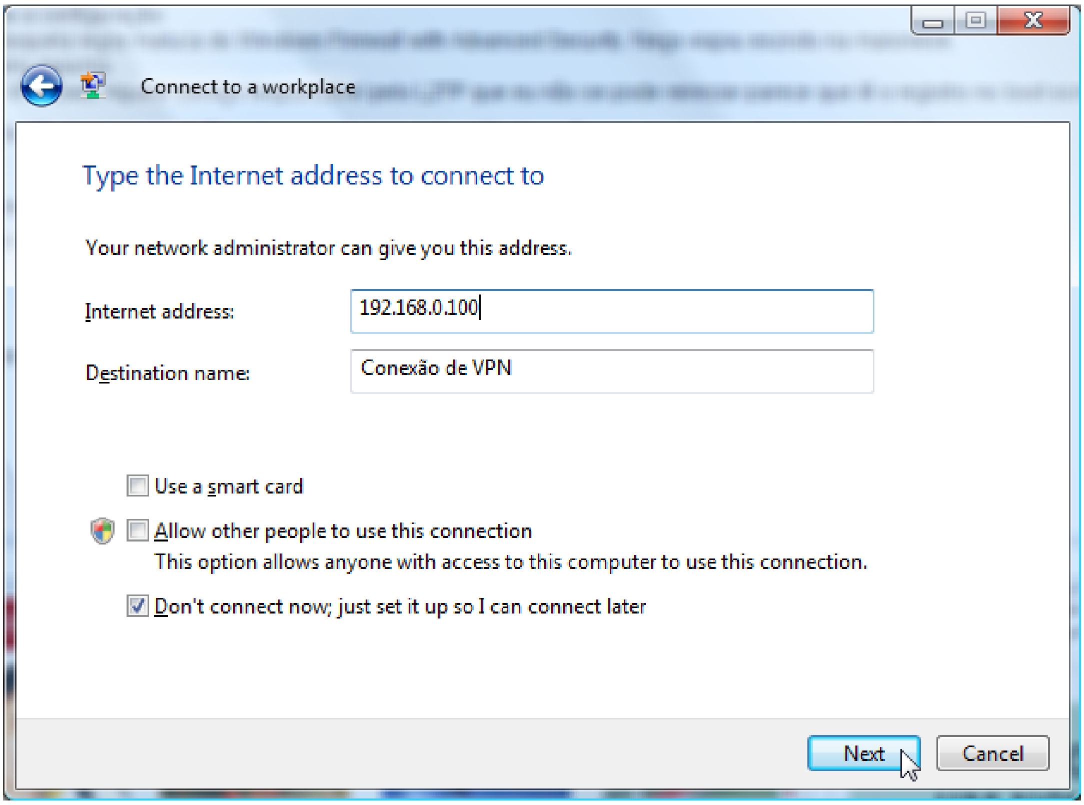
How do you want to connect?

➔ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

➔ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

Image 250 – Configuring the L2TP client (using VPN).



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 192.168.0.100

Destination name: Conexão de VPN

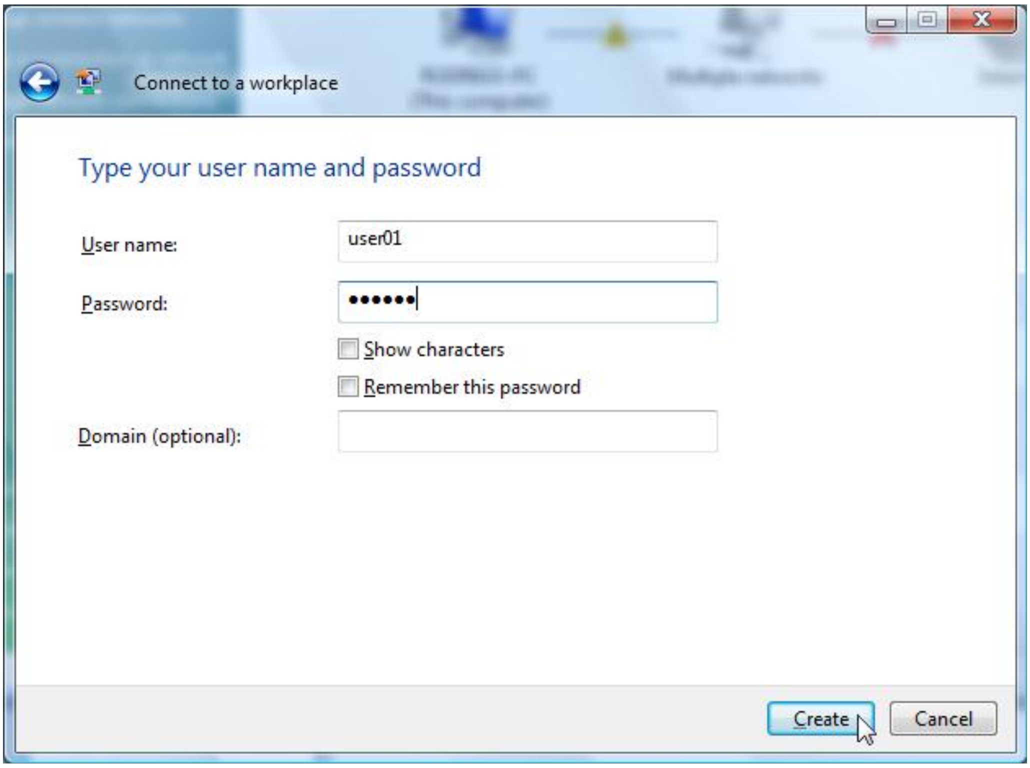
☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

Image 251 – Configuring the L2TP client (Choose the IP and the connection name).

In the image above, 192.168.0.100 is Aker Firewall's address with L2TP server visible by the VPN client. This address can also be a name as *firewall.company.com.*



Type your user name and password

User name: user01

Password: ••••••

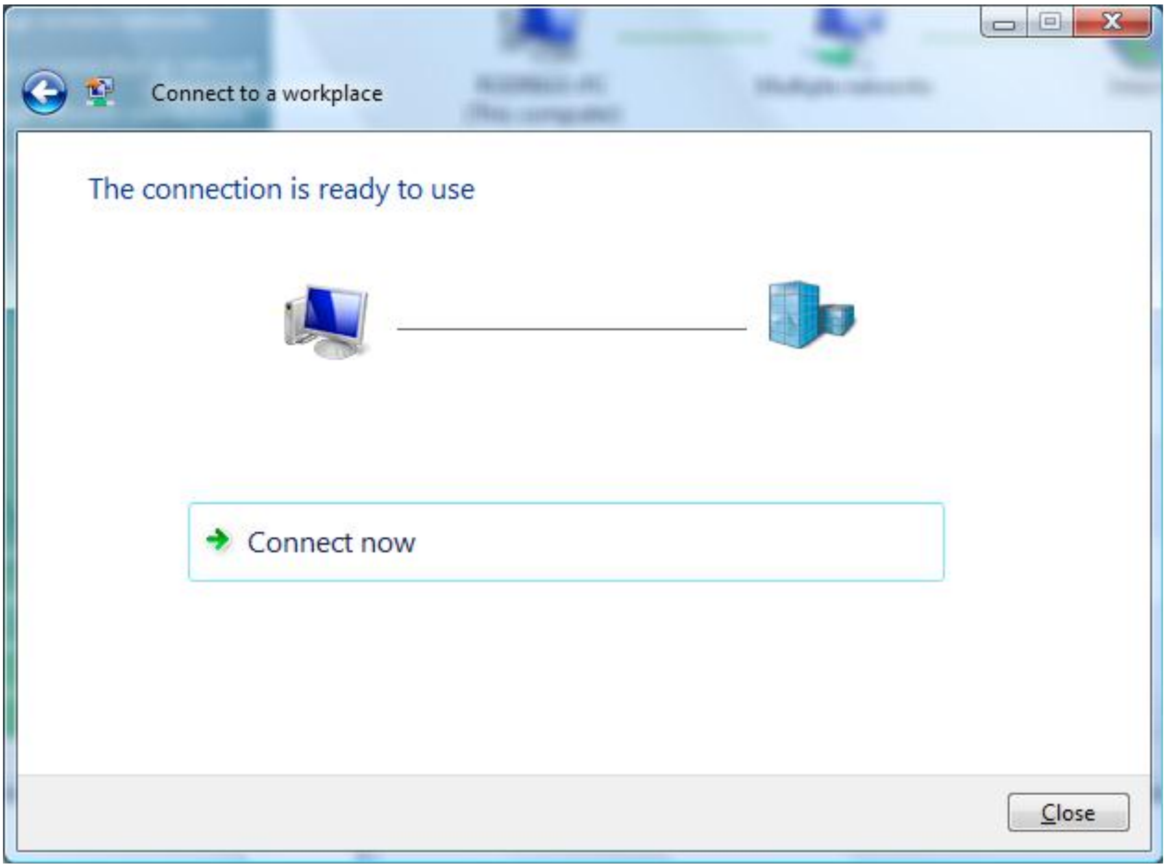
☐ Show characters

☐ Remember this password

Domain (optional):

Image 252 – Configuring the L2TP client (User name and password used to authenticate the VPN client in Aker Firewall).

In the Image above, shall be filled the name and the password that will be used to authenticate the VPN client in Aker Firewall.

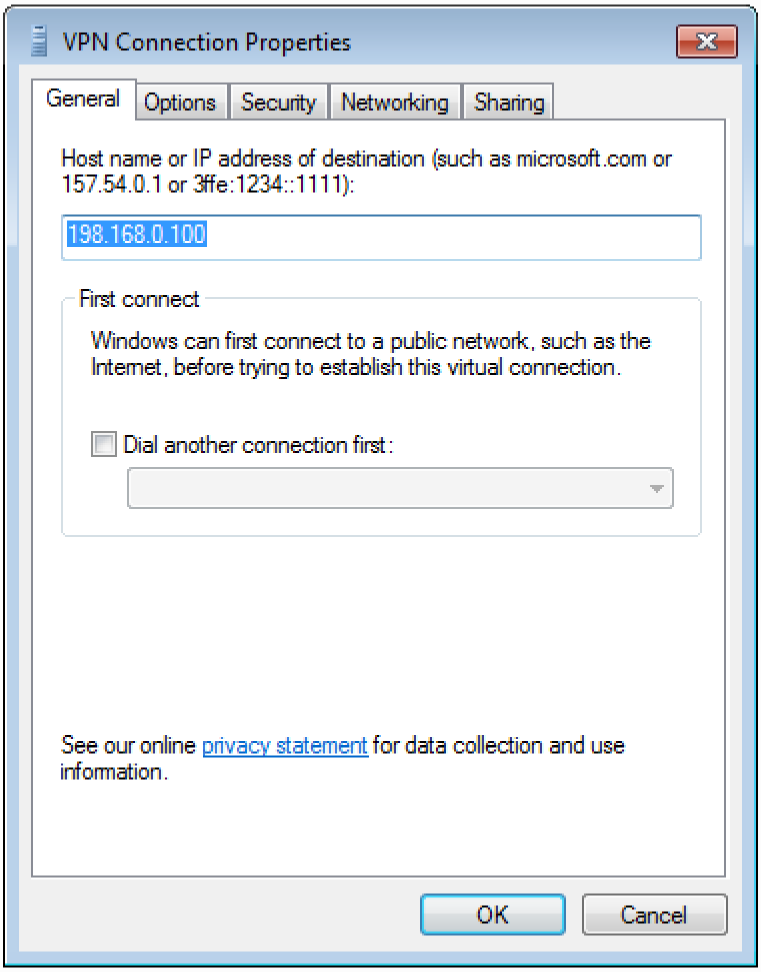

Connect to a workplace
Connect now
Close

The connection is ready to use

Image 253 – VPN L2TP set up has been completed.

After click on *Close*, a new connection will be created, but it need to be configured first, do not click *Connect now* before configuring it.

Go to *Network and Sharing Center*, select *Connect to a network*:



Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

198.168.0.100

First connect

Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.

☐ Dial another connection first:

See our online privacy statement for data collection and use information.

Image 255 – VPN connection properties

Go to VPN Connection Properties, then access the security tab, and configure the window as the Image above:

10.4. PPTP

The ***Point-to-Point Tunneling Protocol*** (***PPTP***) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

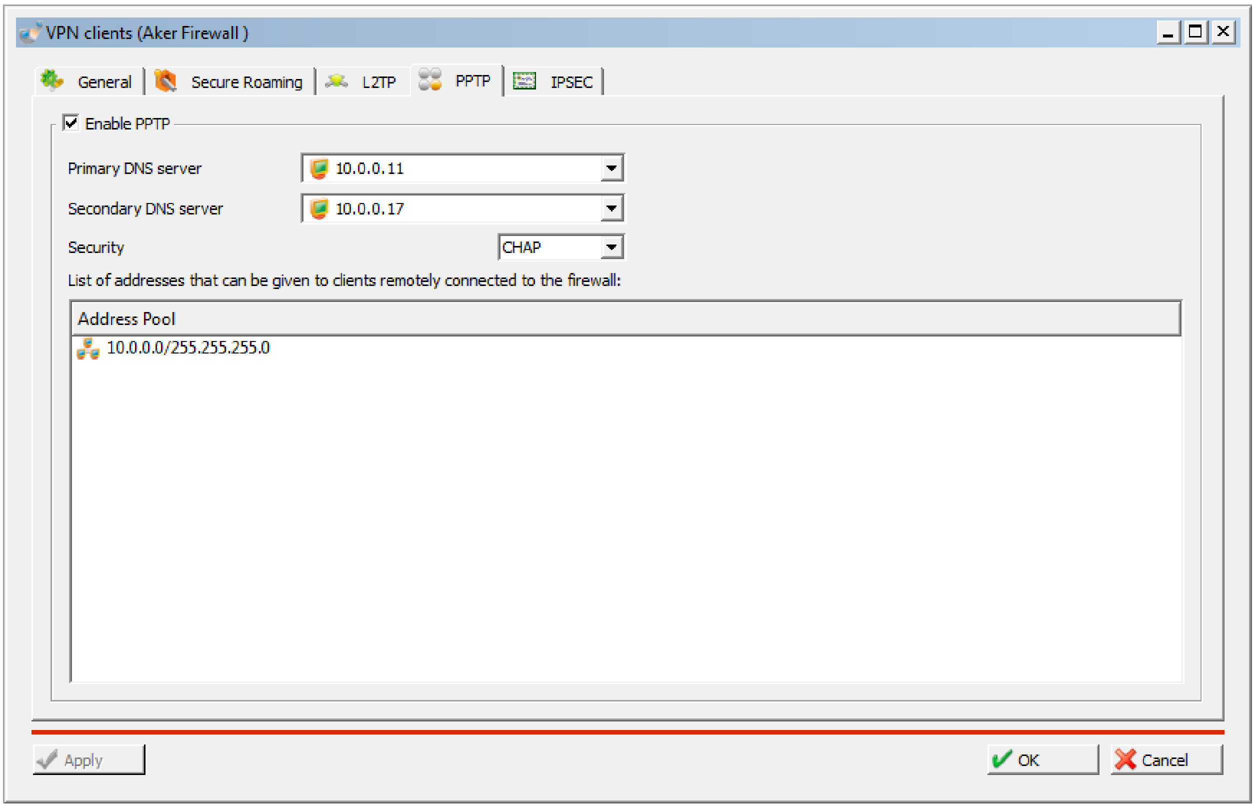
The PPTP specification does not describe encryption or authentication features and relies on the PPP protocol being tunneled to implement security functionality. However the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products.

A *PPTP t*unnel is instantiated by communication to the peer on *TCP port 1723*. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer.

The *PPTP GRE packe*t format is nonstandard, including an additional *acknowledgement* field replacing the typical *routing* field in the GRE header. However, like in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

The GRE tunnel is used to carry encapsulated PPP packets, allowing the tunneling of any protocols that can be carried within PPP, including IP, NetBEUI and IPX

Configuring the VPN PPTP



☑ Enable PPTP

Primary DNS server: 10.0.0.11

Secondary DNS server: 10.0.0.17

Security: CHAP

List of addresses that can be given to clients remotely connected to the firewall:

Address Pool
10.0.0.0/255.255.255.0

Image 254 – Configuring the VPN PPTP

Enable PPTP: This field enables the PPTP server in Aker Firewall and allows configuring other fields such as:

- **Primary and Secondary DNS server:** Configure two DNS servers which will be used during the encryption session. Used in case there is an Internal DNS server in the corporation;
- **Security:** Allow specifying the methods of authentication encryption:
    - **PAP:** Authentication and data not encrypted. It does work with any type of authenticator that can be registered on the Firewall ;

- **CHAP:** Encrypted authentication, data not encrypted. It does work only with the RADIUS authenticator;
- **MS-CHAPv2:** Encrypted authentication, data not encrypted. It does work only with the RADIUS authenticator;
- **MPPE (MS-CHAPv2 + MPPE):** Cypher authentication, encrypted data with RC4 and key from 40 to 128 bits. It works only with RADIUS authenticator;

- **MPPE-128(MS-CHAPv2 + MPPE-128):** Cypher authentication, encrypted data with RC4 and key of 128 bits. It works only with the RADIUS authenticator;

- **Address Pool:** List of addresses that can be assigned to clients connected remotely to the firewall. The addresses installed hosts, all addresses that compose the network, and the included pool, together they add up in order to define the address Pool attributable to clients. Take note that the listed entities must to be connected to any network adapter in the firewall. Otherwise, will not be possible establishing connection with such entity.

  To add an entity to the list, follow the steps bellow:

  - Right-click on the list and select *Add entities*,
    or
  - Drag the entity form the entity field (F5) to the access control list, and drop it there;

  To remove an entity, follow the steps bellow:

  - Right-click on the selected entity, and click on the option *Delete Entities*
    or

  - Select the entity you wish to delete and press the *Delete key* on your keyboard.

  The following Image shows the pop-up menu with all options listed above. You can have access to it right-clicking on any listed entity:

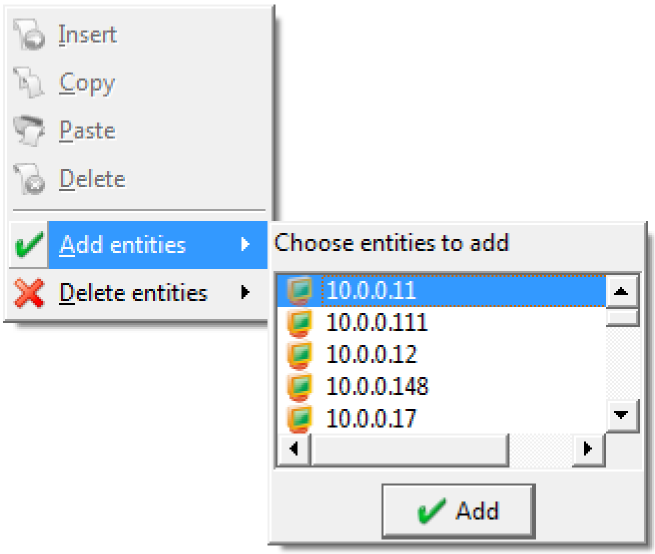

Insert
Copy
Paste
Delete
Add entities
Delete entities
Choose entities to add
10.0.0.11
10.0.0.111
10.0.0.12
10.0.0.148
10.0.0.17
Add

Image 255 – Pop-up menu.

The networks in this field define an address pool, not a subnetwork in sense of *IP routing*. It means, if the firewall's interface is located at subnetwork 10.0.0.0/255.0.0.0 and the network 10.0.0.0/255.255.255.0 is included in the address pool, the first attributable address would be 10.0.0.1 and the last 10.0.0.255. If it were the network 10.1.0.0/255.255.255.0, the range would go from 10.1.0.0 to 10.1.0.255, adding itself in both sides.

Using the text interface

/aker/bin/firewall # fwpptpsrv help

Aker Firewall

Usage: fwpptpsrv help

fwpptpsrv show

fwpptpsrv < enable | disable >

fwpptpsrv clean

fwpptpsrv dns_1 < dns_server >

fwpptpsrv dns_2 < dns_server >

fwpptpsrv add < network >

fwpptpsrv remove < network >

fwpptpsrv security < PAP | CHAP | MS-CHAPv2 | MPPE | MPPE-128 >

The parameters are:

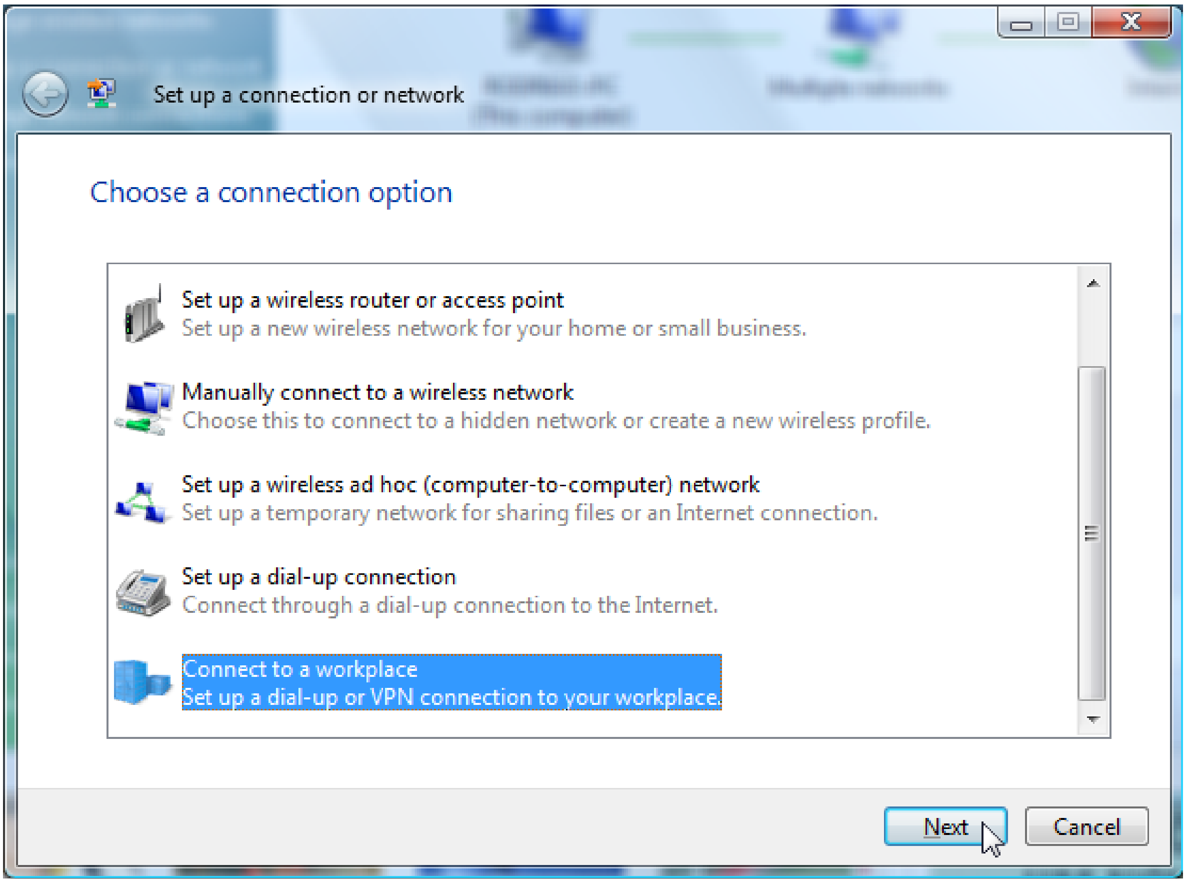
dns_server: A DNS server (entity) for VPN clients

network : Network or host entity for the VPN Clients' IP address pool

Configuring the PPTP Client for authentication with PAP

Windows 7 / XP

On *Windows 7*, you need to create a new VPN connection on *Network and Sharing Center*. On *Windows XP*, it shall be done at the window *Network Connections. A wizard* to assist you in the creation of this connection will be displayed, and must be filled in as described in the Images bellow:



Choose a connection option

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

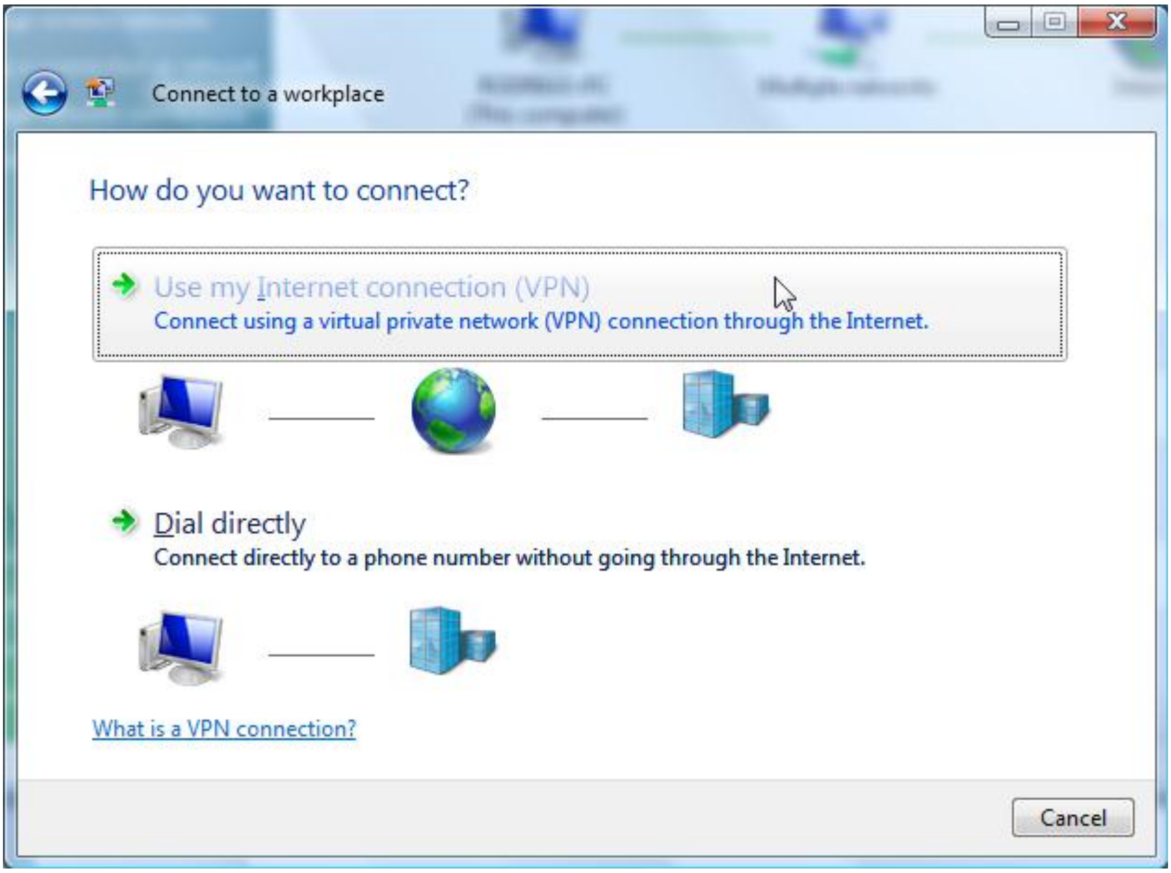
Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.

Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Image 256 – Configuring the PPTP Client for authentication with PAP (Windows Vista/XP).



Connect to a workplace

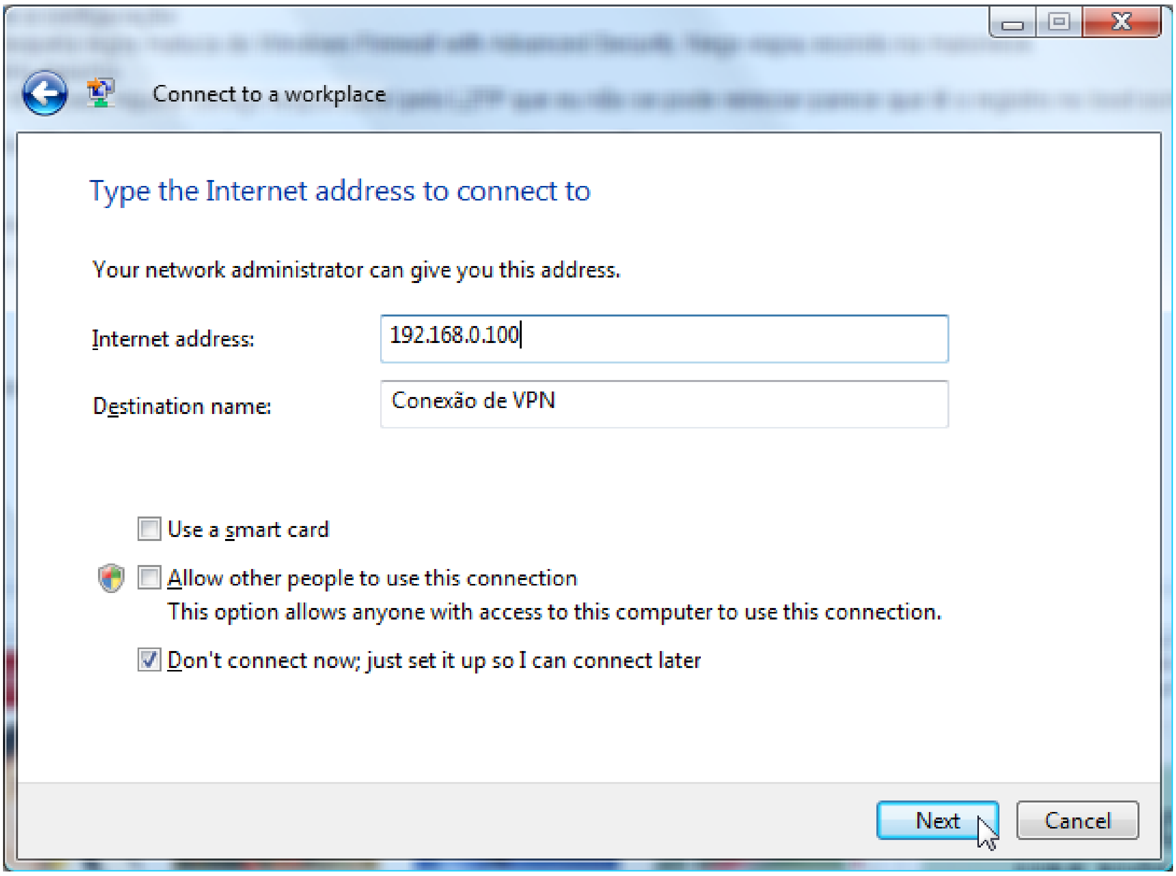
How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

Image 257 – VPN Configuration window on Microsoft Windows ®



Connect to a workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 192.168.0.100

Destination name: Conexão de VPN

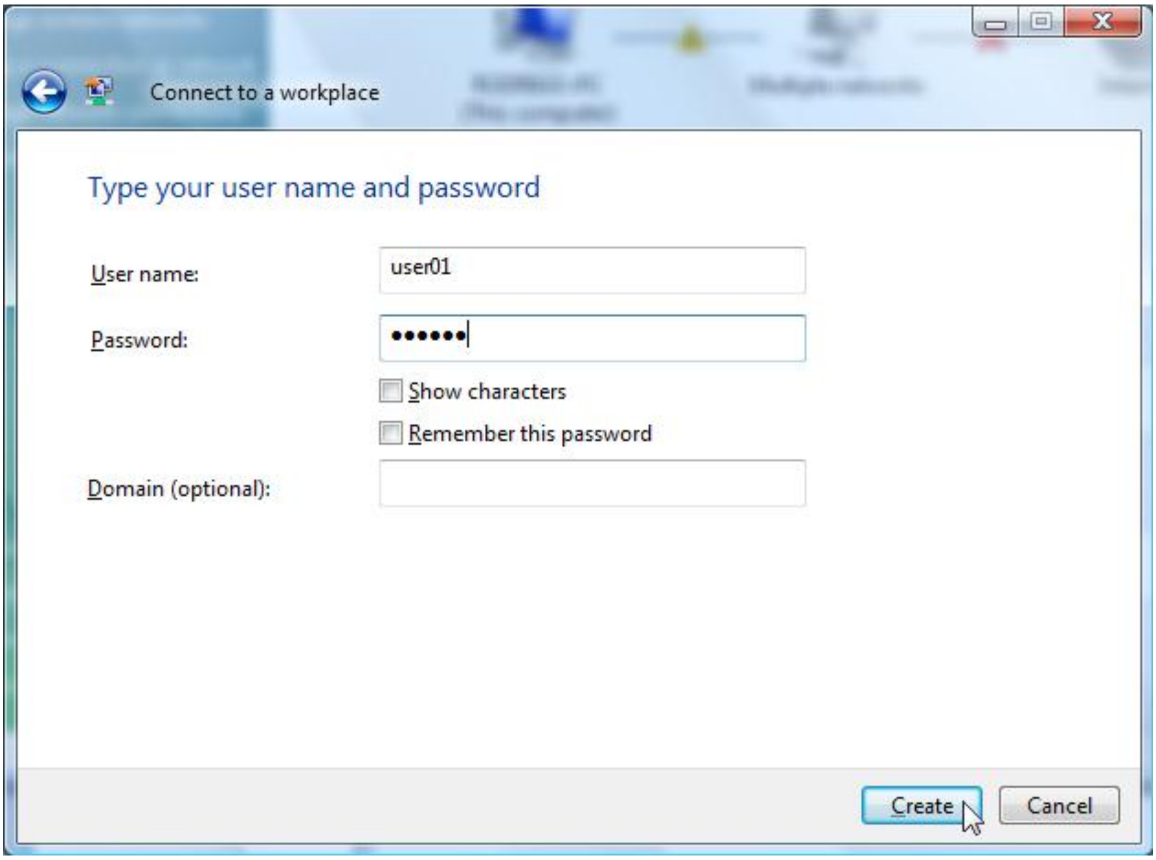
☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

Image 258 – VPN network configuration window on Microsoft Windows®.

In the image above, 192.168.0.100 is Aker Firewall address with the PPTP server visible by the VPN client. The address can also be a name as firewall.company.com.br.



Type your user name and password

User name: user01

Password: ••••••

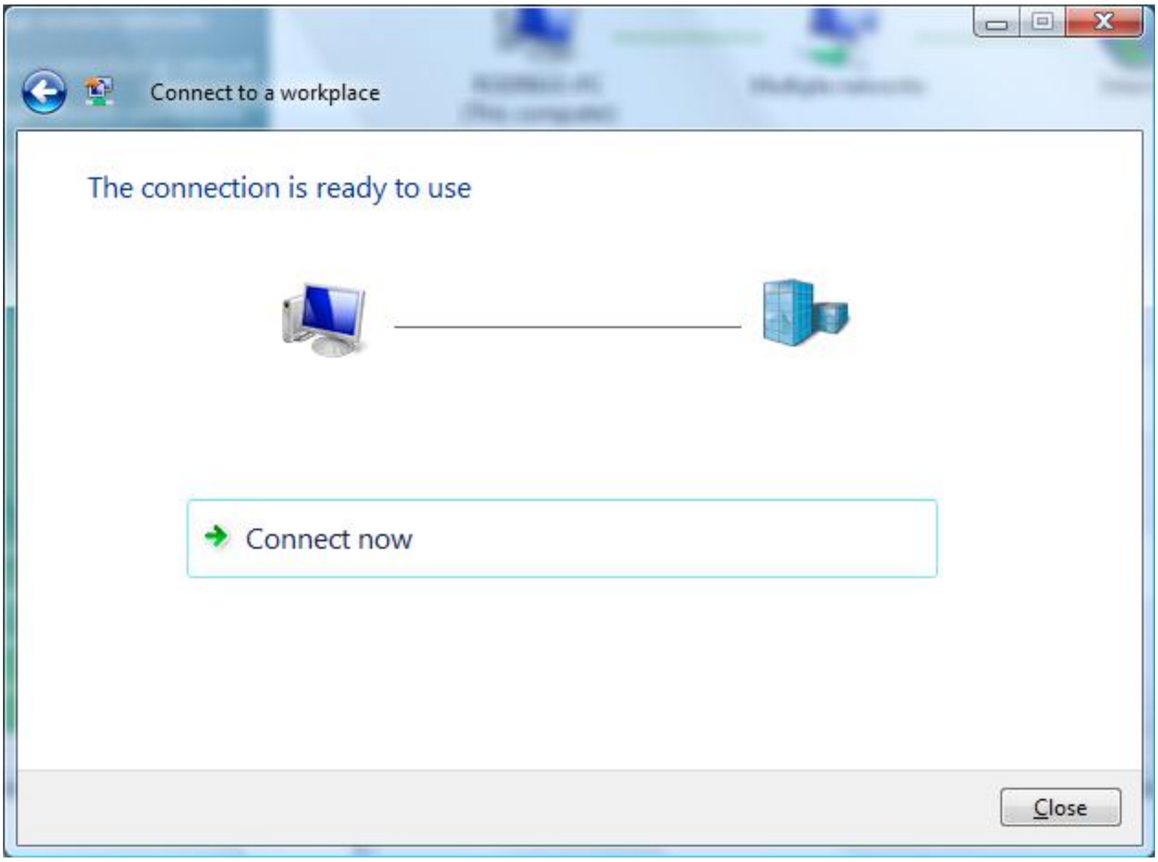
☐ Show characters

☐ Remember this password

Domain (optional):

Image 259 – VPN user name and password configuration window on Microsoft Windows®.

Na imagem acima, devem ser preenchidos o nome de usuário e senha que serão utilizados para autenticar o cliente de VPN no AKER FIREWALL.

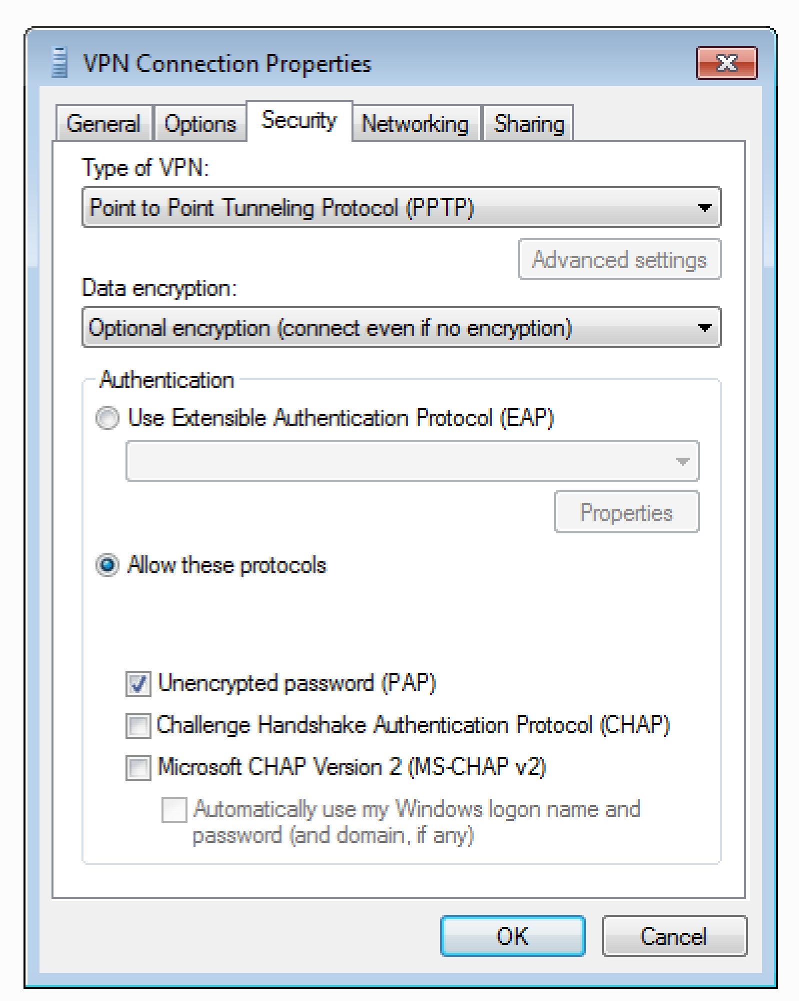

Connect to a workplace
Connect now
Close

The connection is ready to use

Image 260 – VPN configuration on Microsoft Windows® has been completed.

After click on *Close*, a new connection will be created, but it need to be configured first, do not click *Connect now* before configuring it.

Go to *Network and Sharing Center*, select *Connect to a network*:


VPN Connection Properties
General
Options
Security
Networking
Sharing
Advanced settings
Properties
OK
Cancel

Type of VPN:
Point to Point Tunneling Protocol (PPTP)

Data encryption:
Optional encryption (connect even if no encryption)

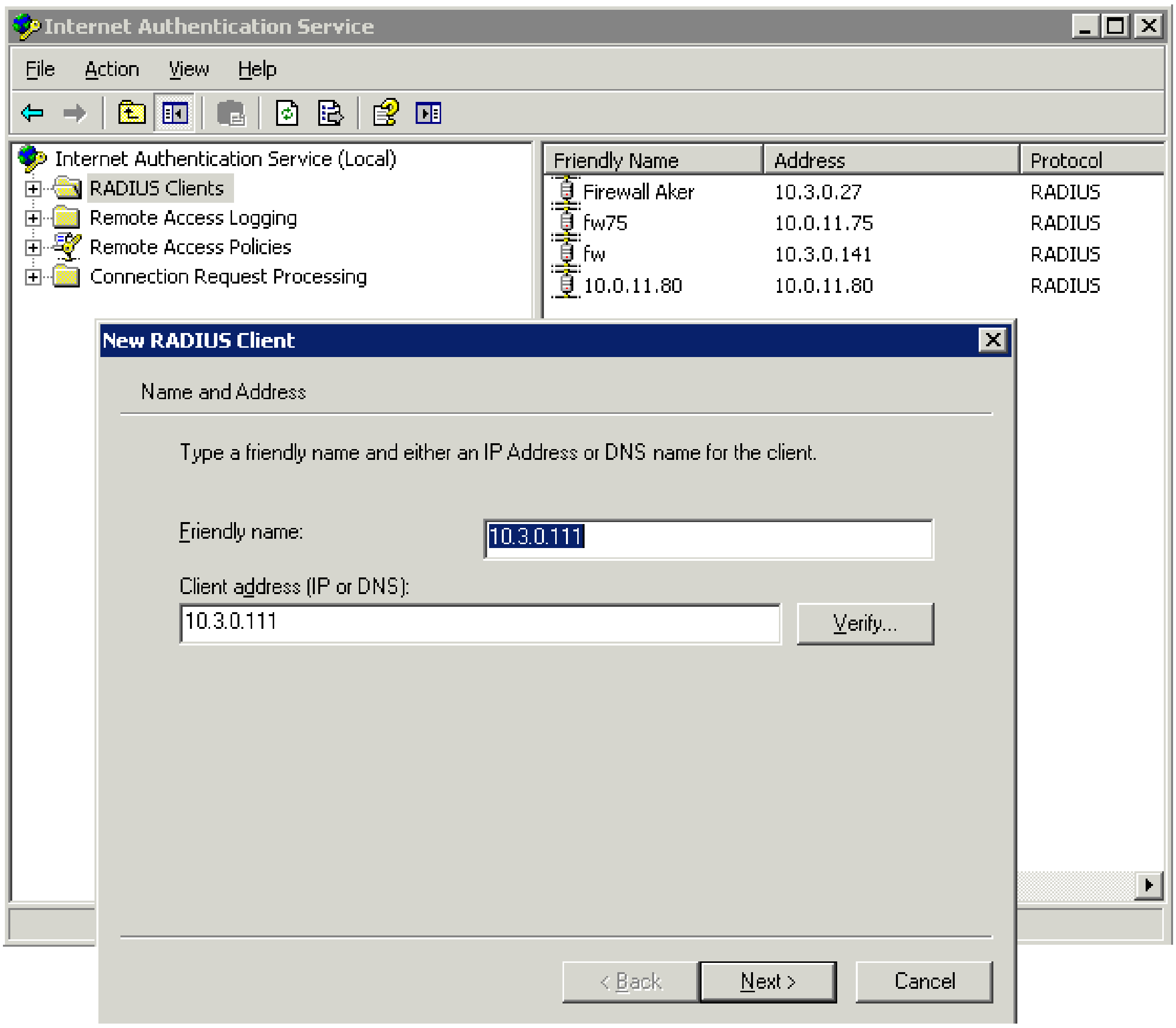
Authentication
○ Use Extensible Authentication Protocol (EAP)
● Allow these protocols
☑ Unencrypted password (PAP)
☐ Challenge Handshake Authentication Protocol (CHAP)
☐ Microsoft CHAP Version 2 (MS-CHAP v2)
☐ Automatically use my Windows logon name and password (and domain, if any)

Image 265 – VPN connection properties

Go to VPN Connection Properties, then access the security tab, and configure the window as the Image above:

Configuring Microsoft Radius Service – IAS

The following configuration accepts all types of encryption. To initiate the setup we need to register the Firewall IP address and its NAS password:


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
New RADIUS Client
Name and Address
Verify...
< Back
Next >
Cancel

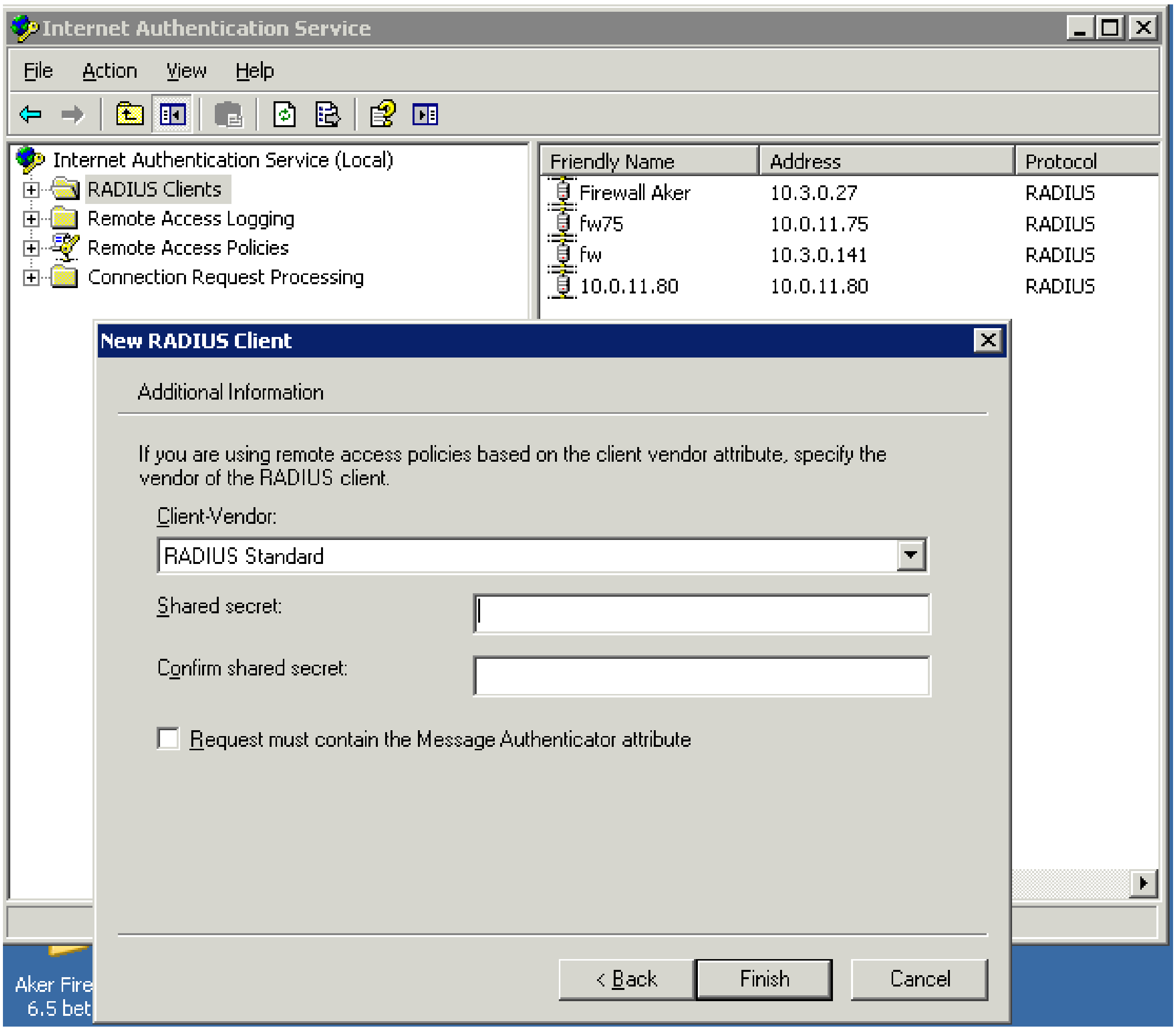
Friendly Name	Address	Protocol
Firewall Aker	10.3.0.27	RADIUS
fw75	10.0.11.75	RADIUS
fw	10.3.0.141	RADIUS
10.0.11.80	10.0.11.80	RADIUS

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: 10.3.0.111

Client address (IP or DNS): 10.3.0.111

Image 261 -Microsoft Server® – *Radius authentication server* name and address.


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
New RADIUS Client
< Back
Finish
Cancel
Aker Fire
6.5 bet

Friendly Name	Address	Protocol
Firewall Aker	10.3.0.27	RADIUS
fw75	10.0.11.75	RADIUS
fw	10.3.0.141	RADIUS
10.0.11.80	10.0.11.80	RADIUS

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

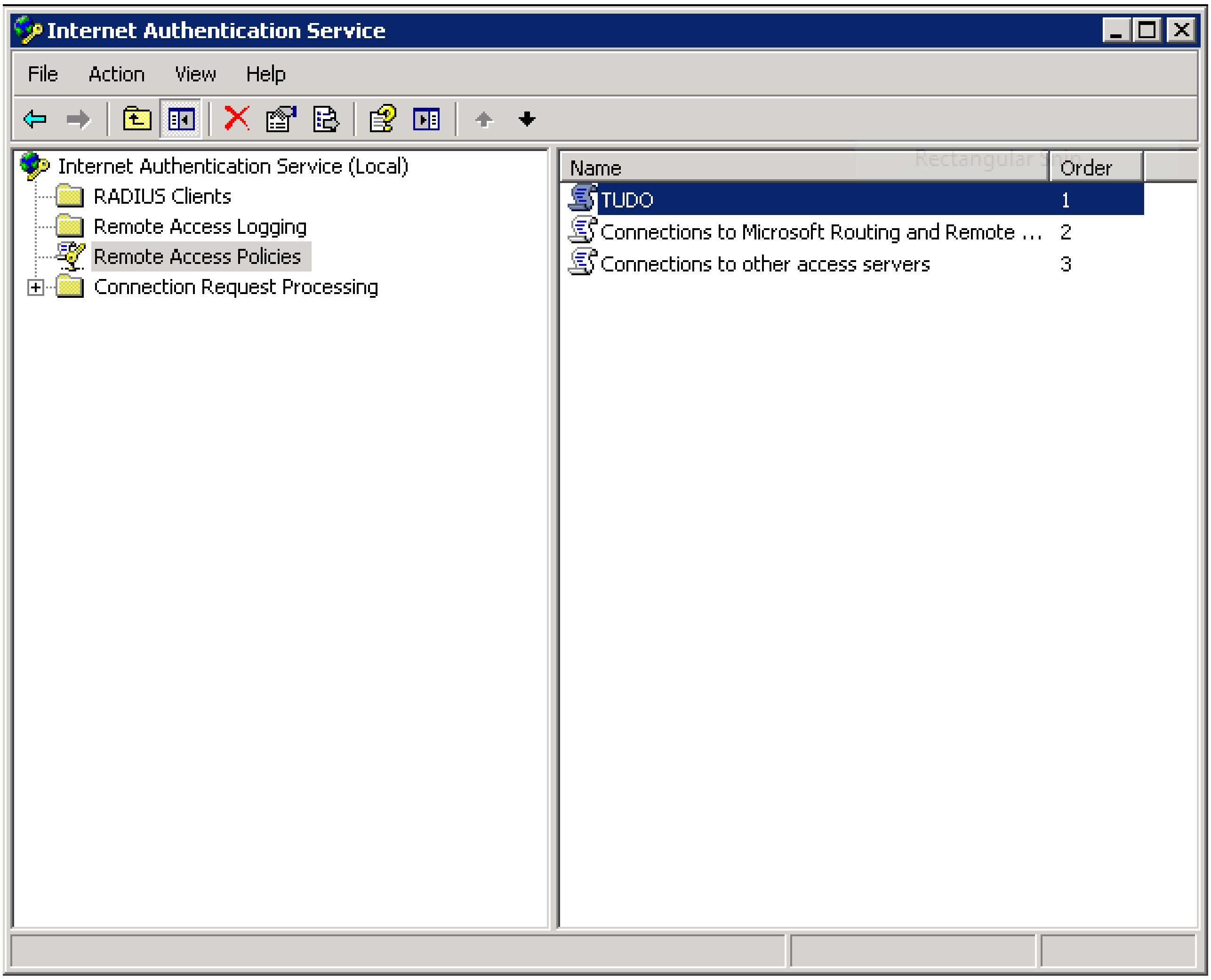
Shared secret:

Confirm shared secret:

☐ Request must contain the Message Authenticator attribute

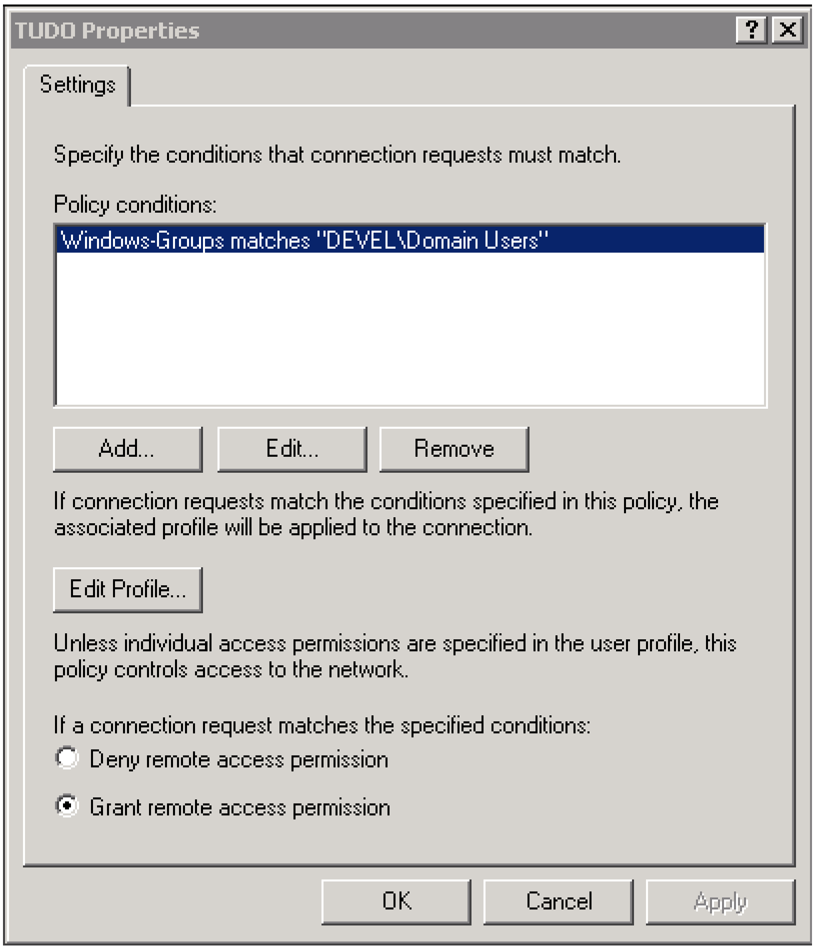
Image 262 – Microsoft Windows Server® -*RADIUS (authenticator server* additional information).

After registering the firewall you have to define the remote access policies:


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Name
Order

Name	Order
TUDO	1
Connections to Microsoft Routing and Remote …	2
Connections to other access servers	3

Image 263 – Microsoft Windows Server® – *RADIUS authenticator server* remote access policies.



TUDO Properties
Settings

Specify the conditions that connection requests must match.

Policy conditions:

Windows-Groups matches "DEVEL\Domain Users"

Add...
Edit...
Remove

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Edit Profile...

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

OK
Cancel
Apply

Image 264 – Microsoft Windows Server® specifying the connections requests conditions.

Click on *Edit Profile*.

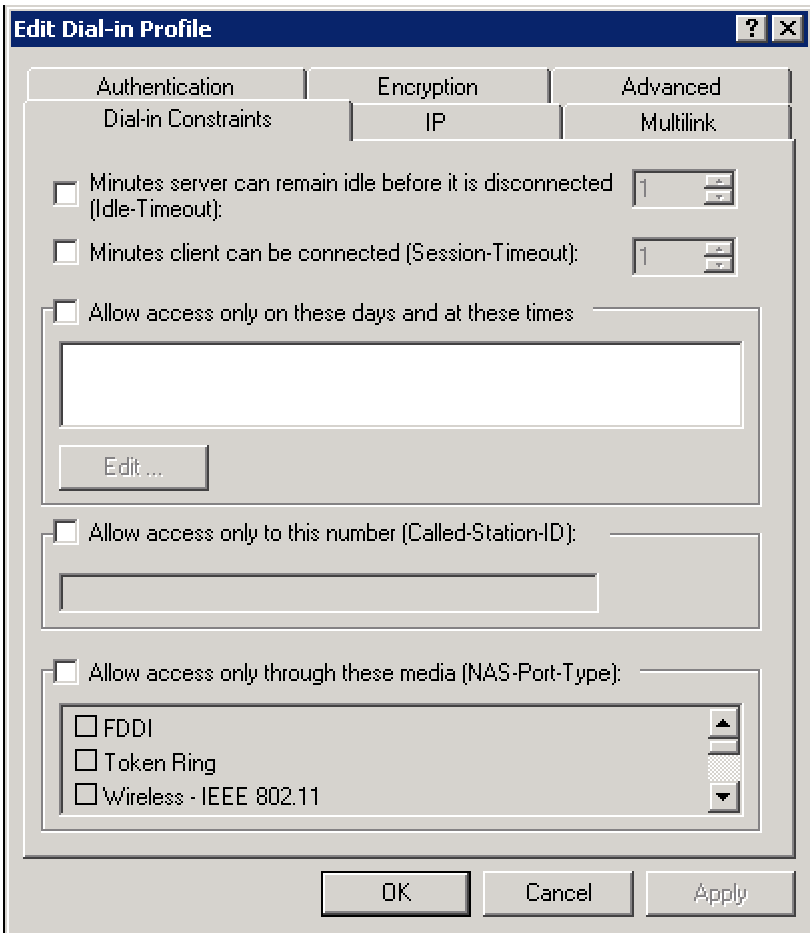
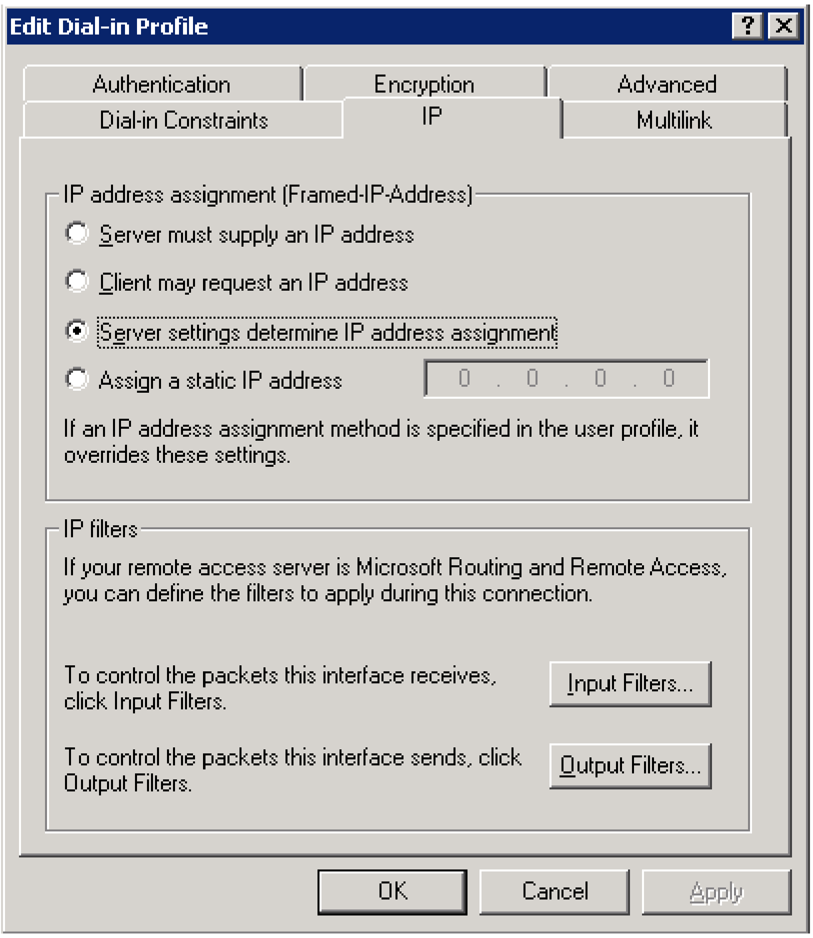

Edit Dial-in Profile
Authentication
Encryption
Advanced
Dial-in Constraints
IP
Multilink
☐ Minutes server can remain idle before it is disconnected (Idle-Timeout): 1
☐ Minutes client can be connected (Session-Timeout): 1
☐ Allow access only on these days and at these times
Edit ...
☐ Allow access only to this number (Called-Station-ID):
☐ Allow access only through these media (NAS-Port-Type):
☐ FDDI
☐ Token Ring
☐ Wireless - IEEE 802.11
OK
Cancel
Apply

Image 265 – Specifying connections conditions – Dial-in Constraints.


Edit Dial-in Profile
?
Authentication
Encryption
Advanced
Dial-in Constraints
IP
Multilink

IP address assignment (Framed-IP-Address)

○ Server must supply an IP address

○ Client may request an IP address

● Server settings determine IP address assignment

○ Assign a static IP address 0 . 0 . 0 . 0

If an IP address assignment method is specified in the user profile, it overrides these settings.

IP filters

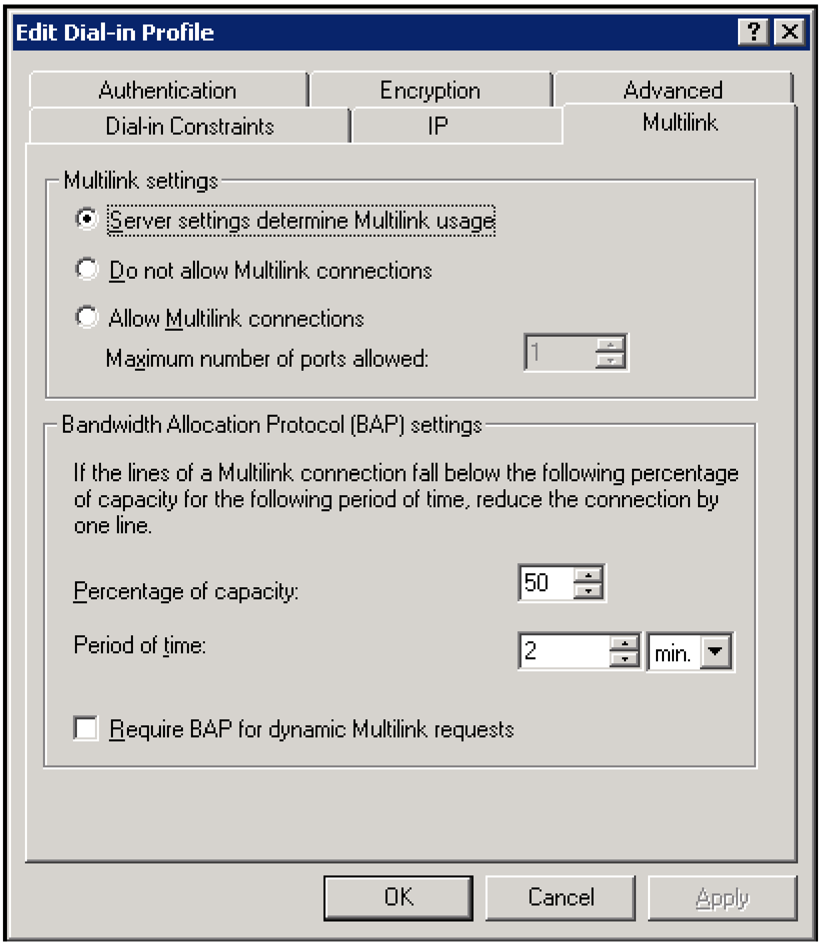
If your remote access server is Microsoft Routing and Remote Access, you can define the filters to apply during this connection.

To control the packets this interface receives, click Input Filters.

To control the packets this interface sends, click Output Filters.

Input Filters...
Output Filters...
OK
Cancel
Apply

Image 266 – Specifying connections conditions – IP.


Edit Dial-in Profile
Authentication
Encryption
Advanced
Dial-in Constraints
IP
Multilink
OK
Cancel
Apply

Multilink settings

● Server settings determine Multilink usage

○ Do not allow Multilink connections

○ Allow Multilink connections

Maximum number of ports allowed: 1

Bandwidth Allocation Protocol (BAP) settings

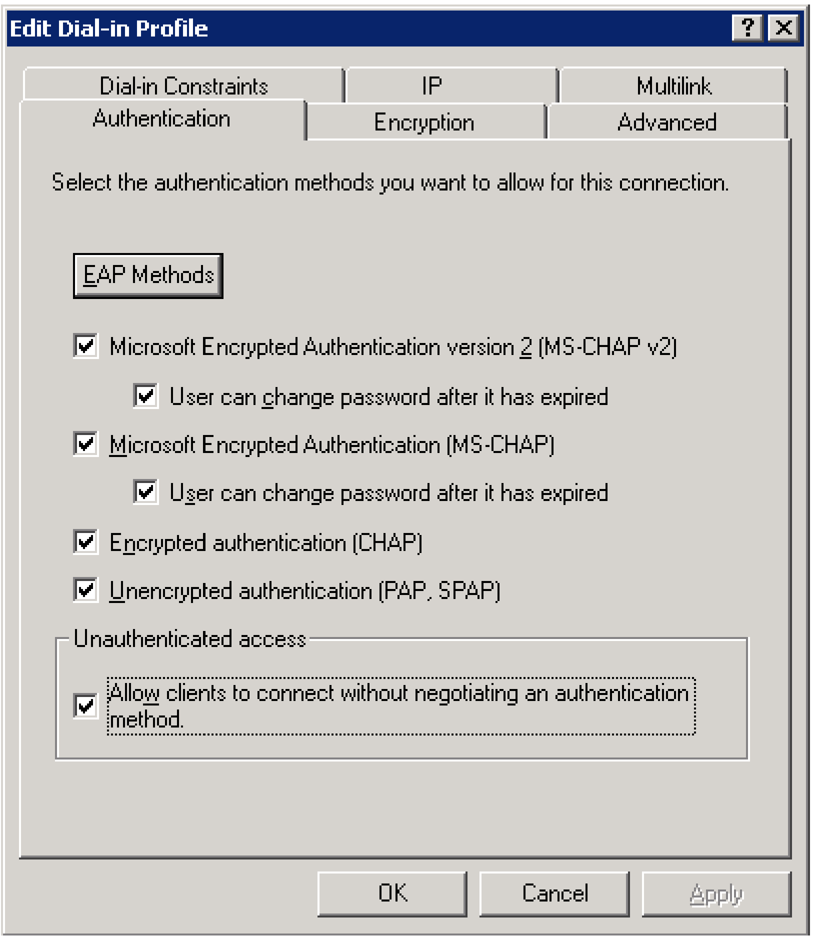
If the lines of a Multilink connection fall below the following percentage of capacity for the following period of time, reduce the connection by one line.

Percentage of capacity: 50

Period of time: 2 min.

☐ Require BAP for dynamic Multilink requests

Image 267 – Specifying connections conditions – Multilink.



Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
EAP Methods
OK
Cancel
Apply

Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

  ☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

  ☑ User can change password after it has expired

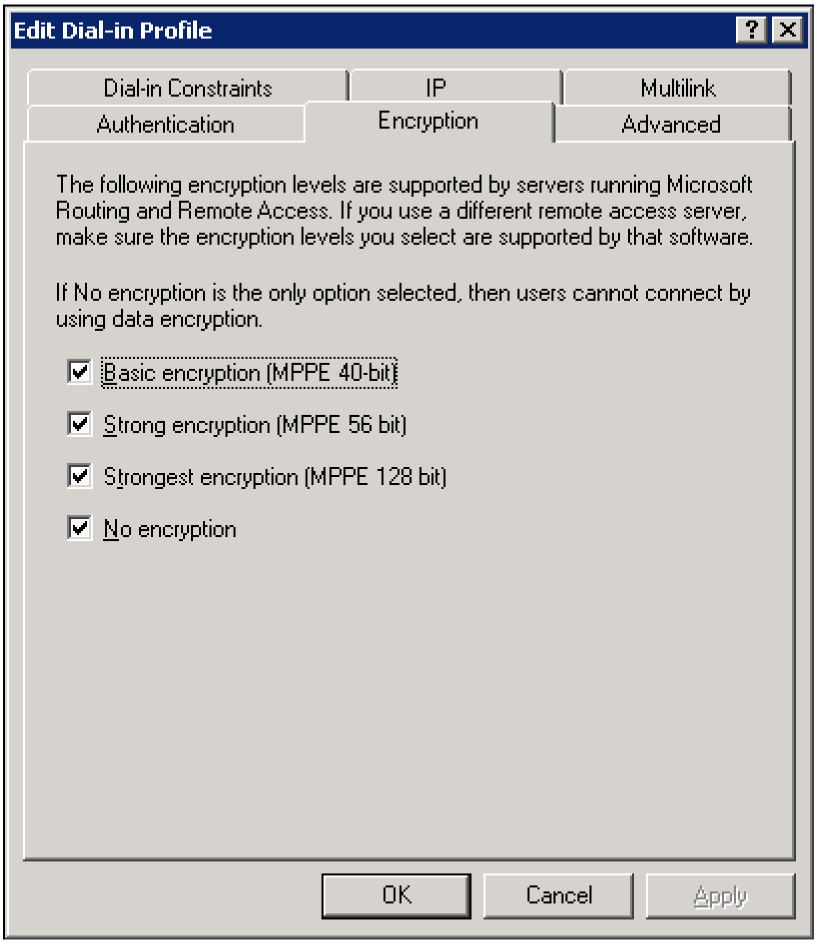
☑ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☑ Allow clients to connect without negotiating an authentication method.

Image 268 – Specifying connections conditions – Authentication.


Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
OK
Cancel
Apply

The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.

If No encryption is the only option selected, then users cannot connect by using data encryption.

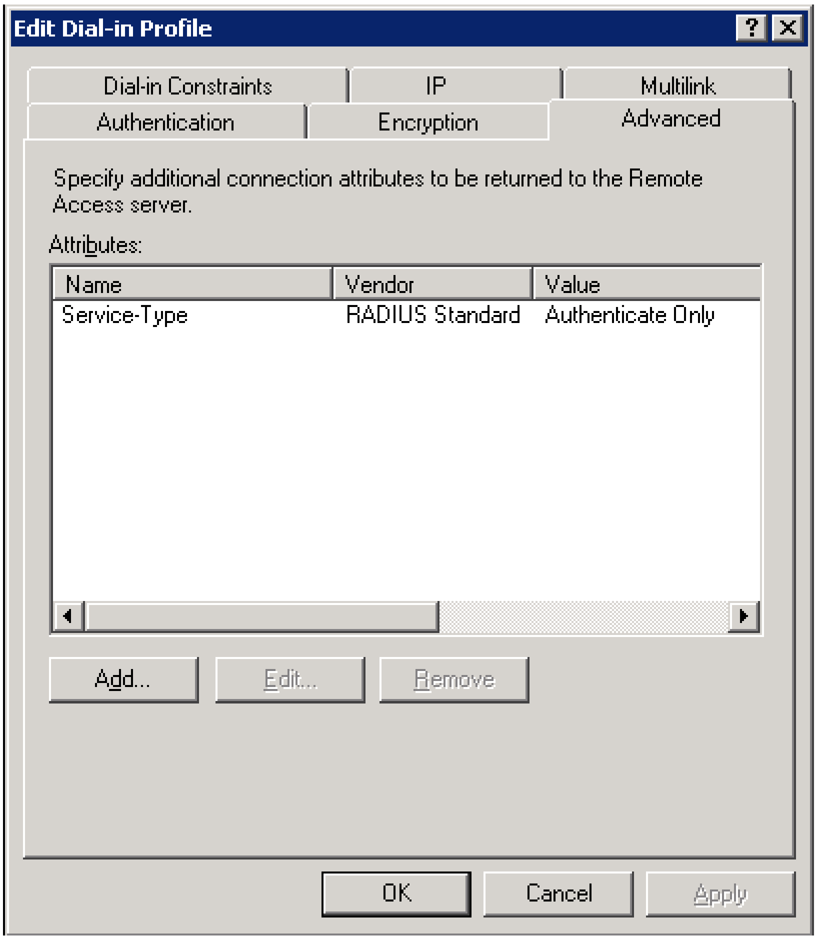
☑ Basic encryption (MPPE 40-bit)

☑ Strong encryption (MPPE 56 bit)

☑ Strongest encryption (MPPE 128 bit)

☑ No encryption

Image 269 – Specifying connections conditions – Encryption.


Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Add...
Edit...
Remove
OK
Cancel
Apply

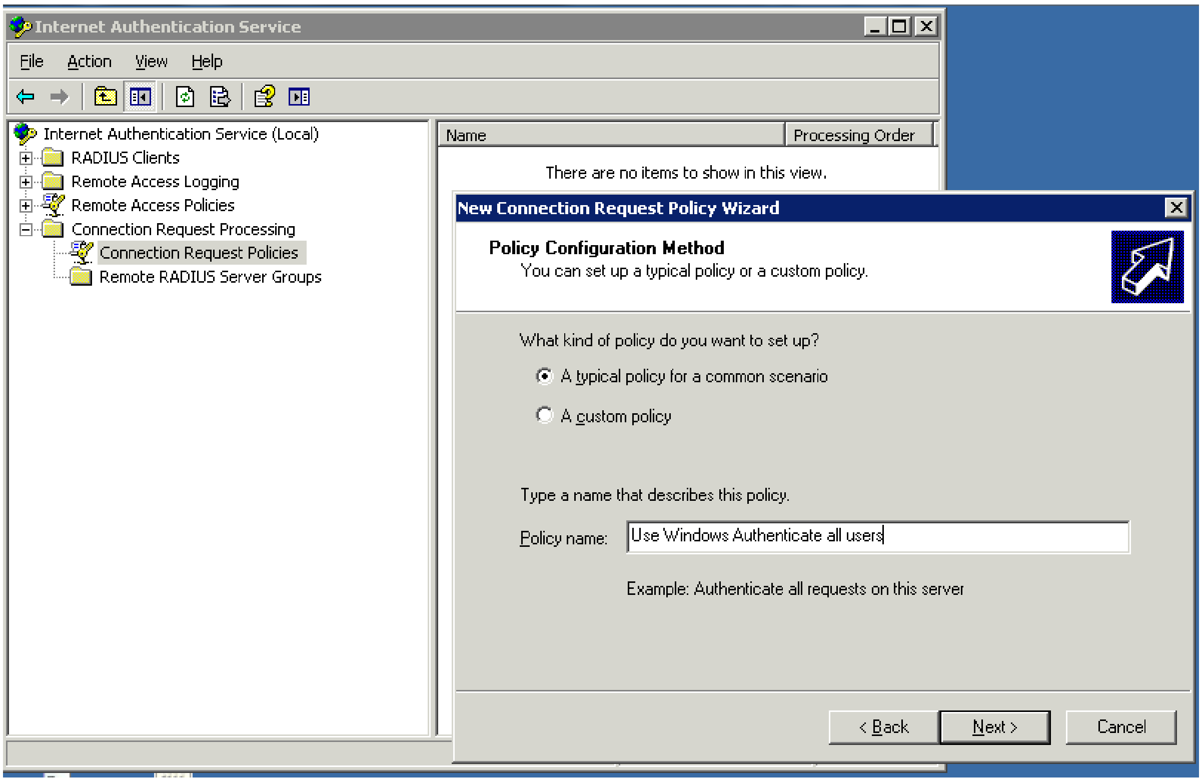
Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Authenticate Only

Image 270 – Specifying connections conditions – Advanced.

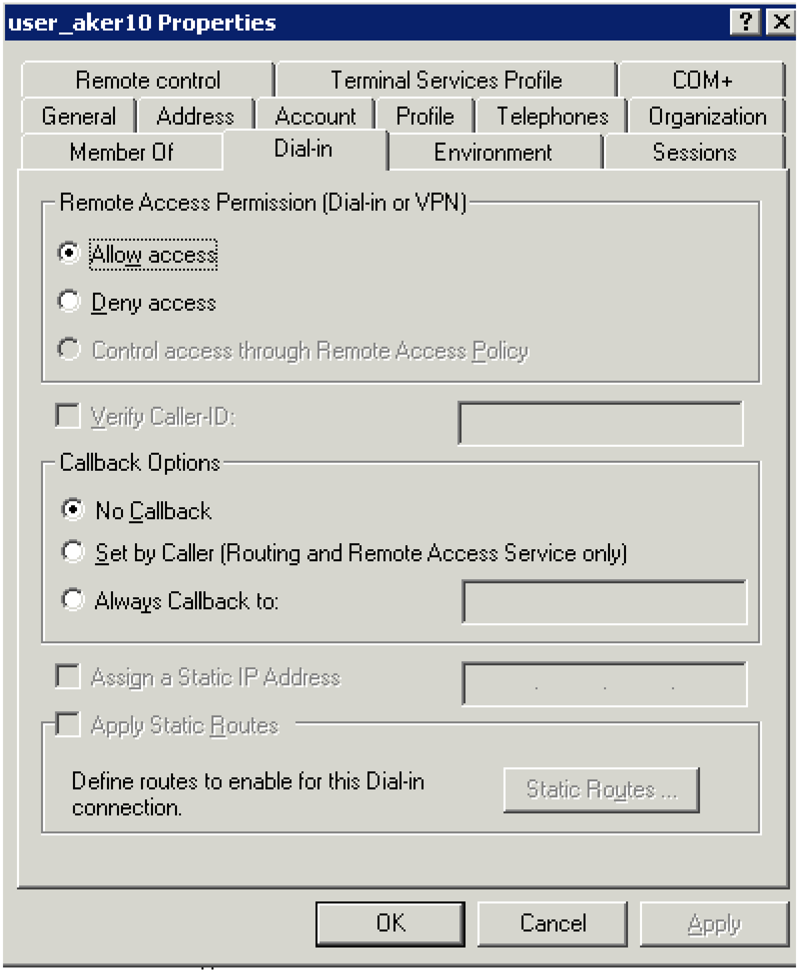
Due to Windows Server security policies, will be necessary to identify which users will be allowed to make this authentications, in order to configure it go to, *Policy* in "*Connection Request Policies*".


Internet Authentication Service
File Action View Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Connection Request Policies
Remote RADIUS Server Groups
Name
Processing Order
There are no items to show in this view.
New Connection Request Policy Wizard
Policy Configuration Method
You can set up a typical policy or a custom policy.
What kind of policy do you want to set up?
● A typical policy for a common scenario
○ A custom policy
Type a name that describes this policy.
Example: Authenticate all requests on this server
< Back
Next >
Cancel

Policy name: Use Windows Authenticate all users

Image 271 – Policy configuration method.

It is also necessary to select the users who may perform the authentications and give them permission to access the VPN and Dial-in, as the example bellow:


user_aker10 Properties
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Static Routes ...
OK
Cancel
Apply

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

☐ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

☐ Assign a Static IP Address

☐ Apply Static Routes

Define routes to enable for this Dial-in connection.

Image 272 – User properties

For CHAP support, it is necessary to change Windows security policies, in order to make it save passwords with reversible encryption, and after change users' passwords.

10.5. IPSEC Client

The IPSEC protocol set (especially IKE and ESP) was not designed for the Client-server mode. Due to it, several extensions in its original implementation (RFC 2401 and family) are necessary so it can be used for this purpose.

Unlike what occurs with the VPNs L2TP/IPSEC and PPTP, there is not a default standard for these necessary extensions for the functioning of VPNs IPSEC tunnel mode for remote clients. There are several RFCs proposals (Internet Drafts) which have never been accepted by the IETF, but even so, they are widely used by various equipment manufactures and VPN clients.

Following, we shall explain several problems found in the establishment of this VPN type and point the solutions, indicating the corresponding RFCs and drafts, if it is the case.

Authentication with user and password

Originally, the IKE protocol supports only the symmetrical authentication, especially using shared secrets or digital certificates. When it comes to VPNs for remote clients, the most practical is use authentication through username and password.

The most common proposal accepted by the IKE is called 1XAUTH, it as a Cisco's proposal which the latest draft is the 2draft-beaulieu-ike-xauth-02. This proposal is widely used by several manufactures and proposes extending the IKE protocol including a second stage of authentication between the traditional phases 1 and 2. With this, after establishing an SA ISAKMP during phase 1, before establishing SAS of phase 2 (ESP), a new encrypted exchange verifies the user's credentials.

Client network configuration

An important problem to be solved in the VPNs IPSEC for clients and its network configuration is; normally the virtual interface is created in the computer where the VPN client is executed and this interface receives addresses and routes from the Intranet protected by the VPNs gateway. In order to do not configure each one of the clients with static IPs address and different, is necessary a solution that allows the VPN server informs the client which configuration is the right one to be used.

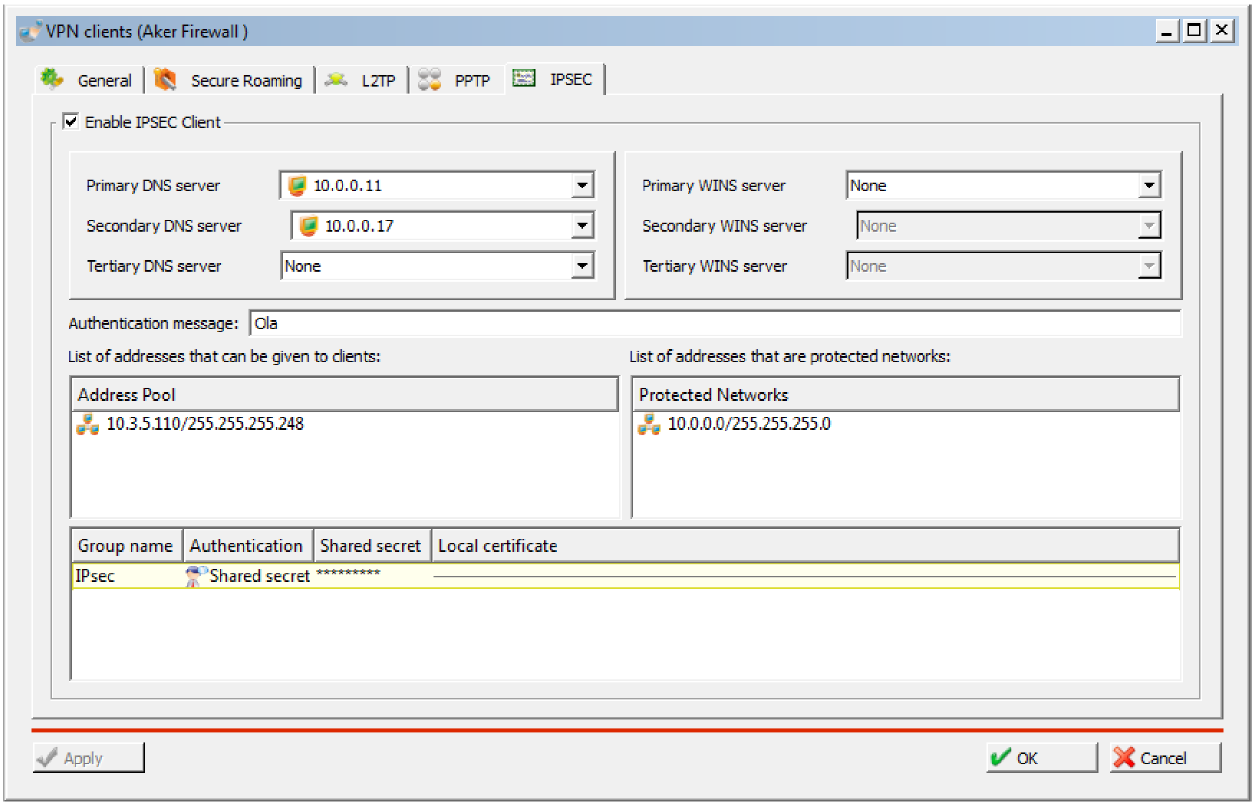
The best proposal to solve this problem is called Mode Config3 also produced by Cisco, and has as latest draft the draftdukes-ike-mode-cfg-024. This proposal is widely used by several VPN equipment manufactures and proposes (same as the XAUTH) between phase 1 and 2, execute a series of questions and answer between encryption client and server.

Disconnected client detection

Remote clients have high probability of being disconnected from the encryption server without prior notice. A simple example is a device connected through WIFI deviates to much from its access point. The IPSEC protocol have no other way of detecting that the connectivity has been lost, which is not the key exchange failure, that happens in long intervals, due to its computational cost.

The default standard for this purpose is described in RFC 3706 and consists in allowing both IPSEC endpoints send ping packets protected by SA phase 1 (ISAKMP) according to its needs. These packets are generally sent in intervals shorter than the key exchange, once all transactions of sending, answering and receiving has a very low cost.

IPSEC



☑ Enable IPSEC Client

Primary DNS server: 10.0.0.11
Secondary DNS server: 10.0.0.17
Tertiary DNS server: None
Primary WINS server: None
Secondary WINS server: None
Tertiary WINS server: None

Authentication message: Ola

List of addresses that can be given to clients:

Address Pool
10.3.5.110/255.255.255.248

List of addresses that are protected networks:

Protected Networks
10.0.0.0/255.255.255.0

Group name	Authentication	Shared secret	Local certificate
IPsec	Shared secret	*********	

Image 273 – VPN clients (IPSEC)

Enable IPSEC Client: This field enable the IPSEC client server in Aker Firewall and allows configuring the other fields as:

- **Primary, secondary and tertiary DNS server:** Configures up to three DNS servers to be used during the encrypted session. Used in case there is an internal DNS server in the corporation;
- **Primary, secondary and tertiary WINS server:** Configures up to three WINS server to be used during the encrypted session. Used in case there is an internal DNS server in the corporation;

- **Authentication message:** Presentation message (banner) that will be displayed to clients.

- **List of address assigned to clients that can be Address Pool:** List of addresses that can be assigned to clients connected remotely to the firewall. The addresses installed hosts, all addresses that compose the network, and the included pool, together, they add up in order to define the address Pool attributable to clients. Take note that the listed entities must to be connected to any network adapter in the firewall. Otherwise, will not be possible establishing connection with such entity.

To add an entity to the list, follow the steps bellow:

- Right-click on the list and select *Add entities*,
  or
- Drag the entity form the entity field (F5) to the access control list, and drop it there;

To remove an entity, follow the steps bellow:

- Right-click on the selected entity, and click on the option *Delete Entities*
  or

- Select the entity you wish to delete and press the *Delete key* on your keyboard.

The following Image shows the pop-up menu with all options listed above. You can have access to it right-clicking on any listed entity:

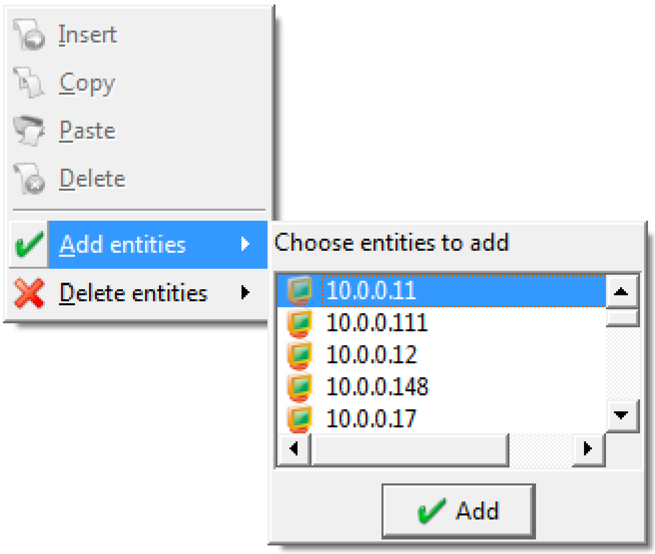


Image 281 – Pop-up menu.

The networks in this field define an address pool, not a subnetwork in sense of *IP routing*. It means, if the firewall's interface is located at subnetwork 10.0.0.0/255.0.0.0 and the network 10.0.0.0/255.255.255.0 is included in the address pool, the first attributable address would be 10.0.0.1 and the last 10.0.0.255. If it were the network 10.1.0.0/255.255.255.0, the range would go from 10.1.0.0 to 10.1.0.255, adding itself in both sides.

- **Protected Network:** List of hosts addresses or networks protected by VPN IPSEC, when used the clients of *VPN IPSEC CLIENT* receive routes to reach these addresses with changing the default gateway of its station. When this field is left in blank the clients of *VPN IPSEC CLIENT* receive Aker Firewall IP address as default gateway.

  To add an entity to the list, follow the steps bellow:

  - Right-click on the list and select *Add entities*,
    Or
  - Drag the entity form the entity field (F5) to the access control list, and drop it there;

  To remove an entity, follow the steps bellow:

  - Right-click on the selected entity, and click on the option *Delete Entities*
    Or
  - Select the entity you wish to delete and press the *Delete key* on your keyboard.

The following Image shows the pop-up menu with all options listed above. You can have access to it right-clicking on any listed entity:

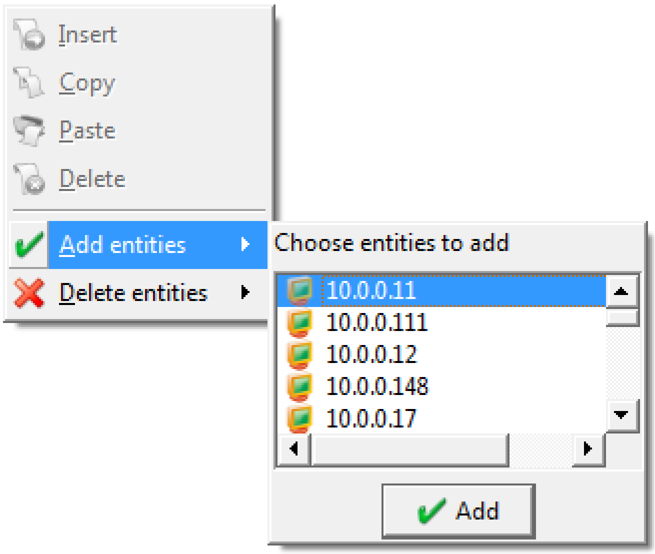

Insert
Copy
Paste
Delete
Add entities
Delete entities
Choose entities to add
10.0.0.11
10.0.0.111
10.0.0.12
10.0.0.148
10.0.0.17
Add

Image 282 – Pop-up menu.

The networks in this field define an address pool, not a subnetwork in sense of *IP routing*. It means, if the firewall's interface is located at subnetwork 10.0.0.0/255.0.0.0 and the network 10.0.0.0/255.255.255.0 is included in the address pool, the first attributable address would be 10.0.0.1 and the last 10.0.0.255. If it were the network 10.1.0.0/255.255.255.0, the range would go from 10.1.0.0 to 10.1.0.255, adding itself in both sides.

Groups: This field allows defining the authentication options of IPSEC for clients:

- **Group name:** Groups identity, the clients specify the group and the authentication method to be used.
- **Authentication:**
  - **Shared secret**: A sequence of character that works as a password and must to be the same in both sides of the tunnel.
  - **Local certificate**: Use X.509 certificates as a public Keys scheme for the firewalls identification. This is the same scheme used for safe websites in the Internet.

Using the text interface

```
/aker/bin/firewall # fwipseccli help

Aker Firewall

Use: fwipseccli help

    fwipseccli show

    fwipseccli < enable | disable > [ group ]

    fwipseccli dns_1 < dns_server >

    fwipseccli dns_2 < dns_server >

    fwipseccli dns_3 < dns_server >

    fwipseccli wins_1 < wins_server >

    fwipseccli wins_2 < wins_server >

    fwipseccli wins_3 < wins_server >

    fwipseccli message < message >

    fwipseccli add < pool | protected > < network >

    fwipseccli remove < pool | protected > < network >

    fwipseccli group < add | remove > < group >

    fwipseccli ss < group > < secret >

    fwipseccli cert < group> < fqdn >

The parameters are:

    Secret    : IPSEC shared secret

    fqdn      : Domain name presented in the X.509 certificate for IPSEC
authentication


    dns_server : A DNS server (entity) for VPN clients
```

wins_server: A WINS server (entity) for VPN clients

network : Network or host entity for the VPN Clients' IP address pool or the list of protected network

group : Clients' group name

message : User authentication message

Configuring the Clients

Generally, the recommended configurations for encryption clients are the following:

Shared Secret

Phase	Configuration	Value
1	Authentication form	secret + XAUTH
1	Identification form	KEY_ID. Use the same group name created in the fwipseccli. Some clients call this configuration *Group*.
1	User credential (XAUTH)	Use username and password that can be verified by the Aker Firewall authentication subsystem, the same, as example, the one that the *Web Filtering* accepts for the authentication.
1	Encryption algorithm and hash	3DES / SHA-1 (can be modified by the Control Center)
1	Diffie-hellman group	2 – MODP-1024 (can be modified by the Control Center)
1	SA lifetime	3600 seconds (can be modified by the Control Center)
2	Algorithm	AES-256 / SHA-1 HMAC-96
2	PFS / Diffie hellman group	No / 0
2	AS lifetime	3600 seconds

Image 274 – Recommended configuration for encryption clients (Shared Secret)

X.509

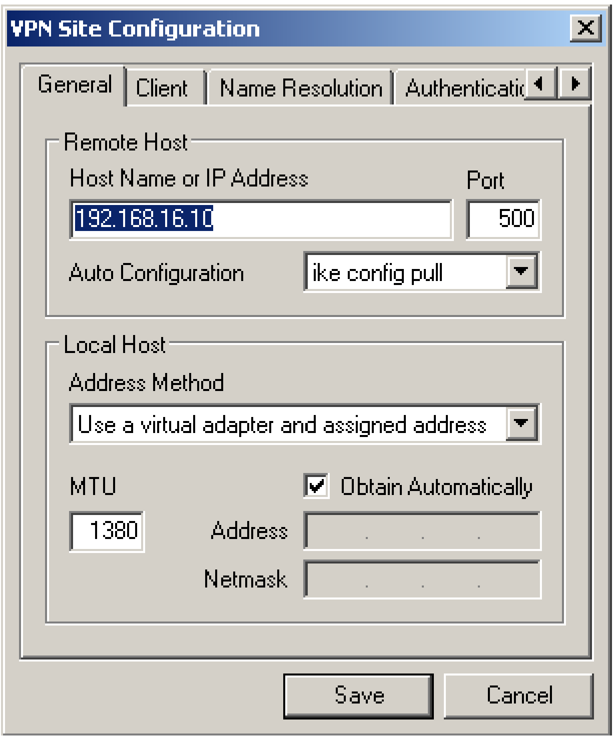
X.509 is very similar with the one above:

Phase	Configuration	Value
1	Authentication form	X.509 (RSA SIG) + XAUTH.
1	Identification form	FQDN. Use the certificate Subject Alternative Name. Some clients demand this name to be the same as the IP address or domain connection name.
1	User credential (XAUTH)	Use username and password that can be verified by the Aker Firewall authentication subsystem, the same, as example, the one that the *Web Filtering* accepts for the authentication.
1	Encryption algorithm and hash	3DES / SHA-1 (can be modified by the Control Center)
1	Diffie-hellman group	2 – MODP-1024 (can be modified by the Control Center)
1	SA lifetime	3600 seconds (can be modified by the Control Center)
2	Algorithm	AES-256 / SHA-1 HMAC-96
2	PFS / Diffie hellman Group	No / 0
2	SA lifetime	3600 seconds

Image 275 – Recommended configuration for encryption clients (X.509)

Examples:

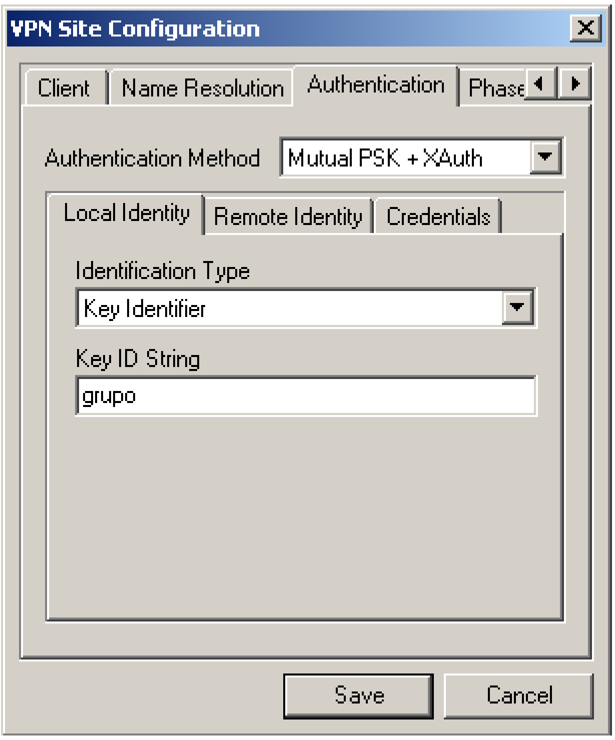
ShrewSoft VPN Client with shared secret


VPN Site Configuration
General
Client
Name Resolution
Authenticatio
Save
Cancel

Remote Host
Host Name or IP Address: 192.168.16.10
Port: 500
Auto Configuration: ike config pull

Local Host
Address Method: Use a virtual adapter and assigned address
MTU: 1380
☑ Obtain Automatically
Address: . . .
Netmask: . . .

Image 276 – VPN configuration (General)

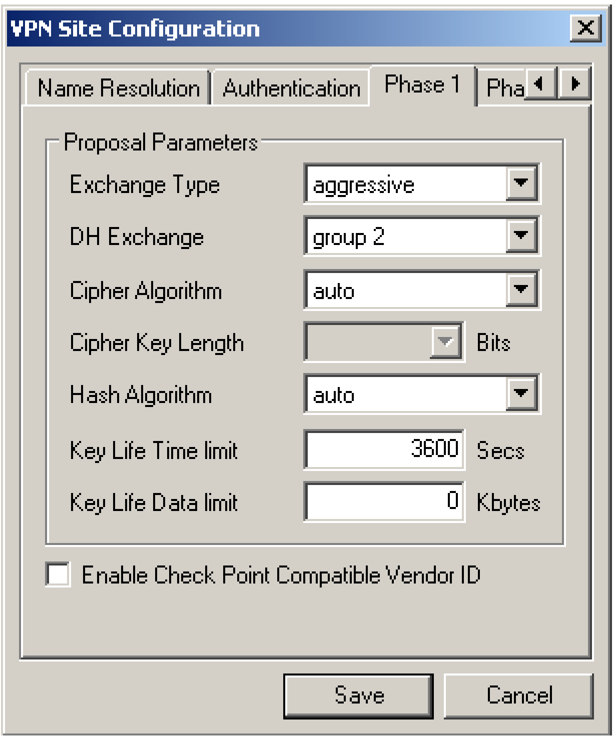

VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Local Identity
Remote Identity
Credentials
Save
Cancel

Authentication Method: Mutual PSK + XAuth

Identification Type: Key Identifier

Key ID String: grupo

Image 277 – VPN configuration (Authentication)


VPN Site Configuration
Name Resolution
Authentication
Phase 1
Pha
Proposal Parameters
Save
Cancel

Exchange Type: aggressive

DH Exchange: group 2

Cipher Algorithm: auto

Cipher Key Length: Bits

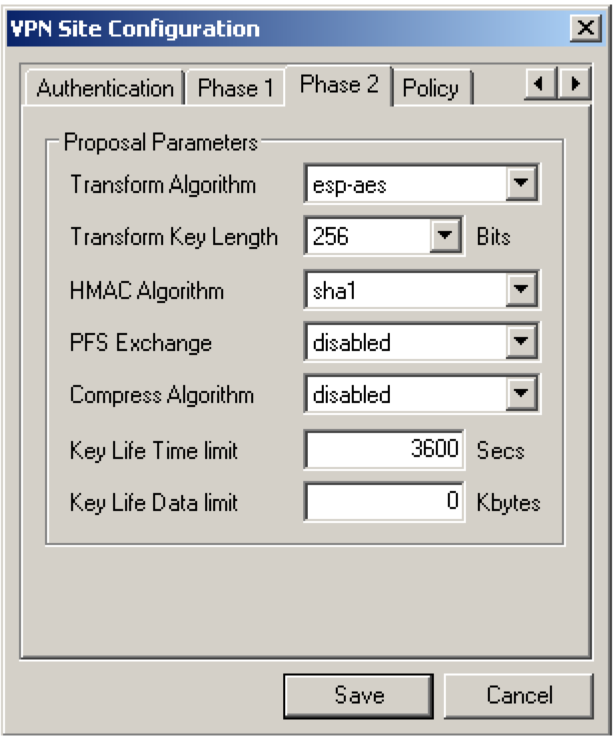
Hash Algorithm: auto

Key Life Time limit: 3600 Secs

Key Life Data limit: 0 Kbytes

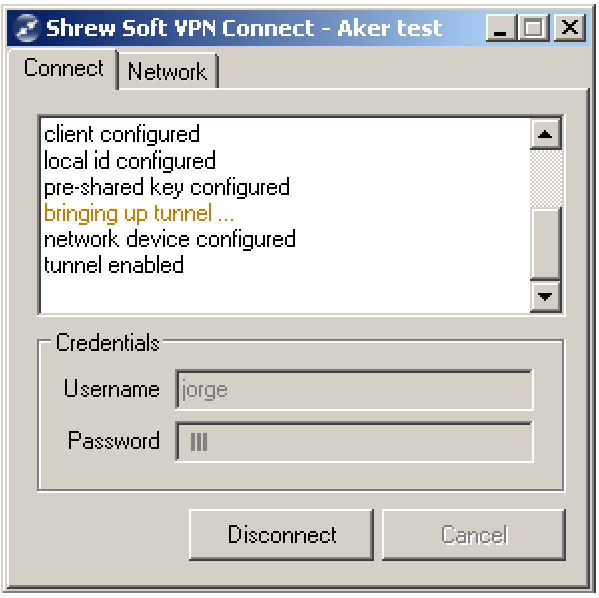
☐ Enable Check Point Compatible Vendor ID

Image 278 – VPN configuration (Phase 1)


VPN Site Configuration
Authentication
Phase 1
Phase 2
Policy
Proposal Parameters
Save
Cancel

Transform Algorithm: esp-aes
Transform Key Length: 256 Bits
HMAC Algorithm: sha1
PFS Exchange: disabled
Compress Algorithm: disabled
Key Life Time limit: 3600 Secs
Key Life Data limit: 0 Kbytes

Image 279 – VPN configuration (Phase 2)


Shrew Soft VPN Connect - Aker test
Connect
Network
Credentials
Disconnect
Cancel

```
client configured
local id configured
pre-shared key configured
bringing up tunnel ...
network device configured
tunnel enabled
```

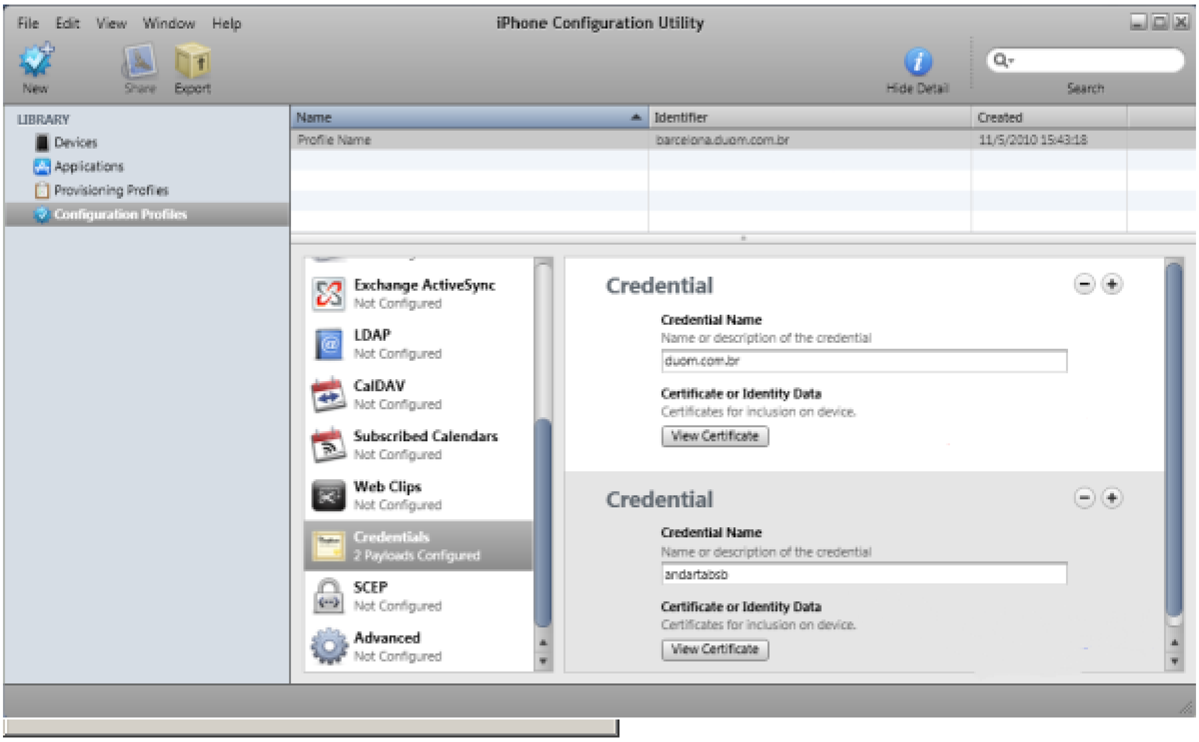
Username: jorge
Password: |||

Image 280 – VPN configuration (Connect)

IPhone with certificate

In this case is necessary to use the configuration tool for IPhone companies. This tool can be acquired free at Apple’s website. It is necessary to include the CA certificate (CER) and the certificate with client keys (.PFX) in the configuration profile. To do it, first is necessary to include these certificates in the Windows configurations.

IPhone requires the “Hostname or IP Address for Server” be the same as the Subject Alternative do firewall, under penalty of refuses the certificate and block the connection.


File
Edit
View
Window
Help
iPhone Configuration Utility
New
Share
Export
Hide Detail
Search
LIBRARY
Devices
Applications
Provisioning Profiles
Configuration Profiles
Exchange ActiveSync
Not Configured
LDAP
Not Configured
CalDAV
Not Configured
Subscribed Calendars
Not Configured
Web Clips
Not Configured
Credentials
2 Payloads Configured
SCEP
Not Configured
Advanced
Not Configured
View Certificate
View Certificate

Name	Identifier	Created
Profile Name	barcelona.duom.com.br	11/5/2010 15:43:18

Credential

Credential Name
Name or description of the credential
duom.com.br

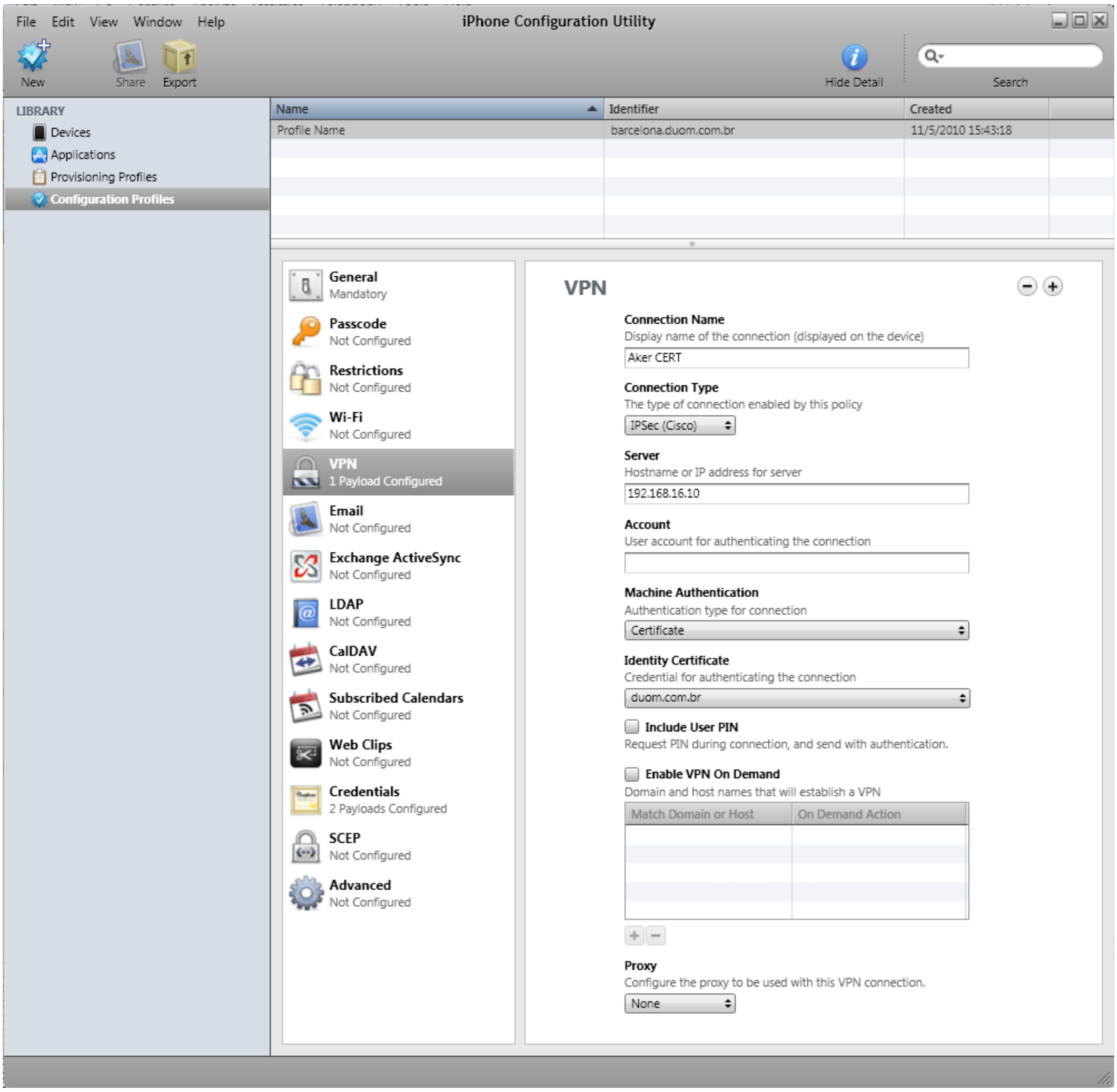
Certificate or Identity Data
Certificates for inclusion on device.

Credential

Credential Name
Name or description of the credential
andartabsb

Certificate or Identity Data
Certificates for inclusion on device.

Image 281 – IPhone configuration (certificate)


File
Edit
View
Window
Help
iPhone Configuration Utility
New
Share
Export
Hide Detail
Search
LIBRARY
Devices
Applications
Provisioning Profiles
Configuration Profiles
General
Mandatory
Passcode
Not Configured
Restrictions
Not Configured
Wi-Fi
Not Configured
VPN
1 Payload Configured
Email
Not Configured
Exchange ActiveSync
Not Configured
LDAP
Not Configured
CalDAV
Not Configured
Subscribed Calendars
Not Configured
Web Clips
Not Configured
Credentials
2 Payloads Configured
SCEP
Not Configured
Advanced
Not Configured
Match Domain or Host
On Demand Action

Name	Identifier	Created
Profile Name	barcelona.duom.com.br	11/5/2010 15:43:18

VPN

Connection Name
Display name of the connection (displayed on the device)
Aker CERT

Connection Type
The type of connection enabled by this policy
IPSec (Cisco)

Server
Hostname or IP address for server
192.168.16.10

Account
User account for authenticating the connection

Machine Authentication
Authentication type for connection
Certificate

Identity Certificate
Credential for authenticating the connection
duom.com.br

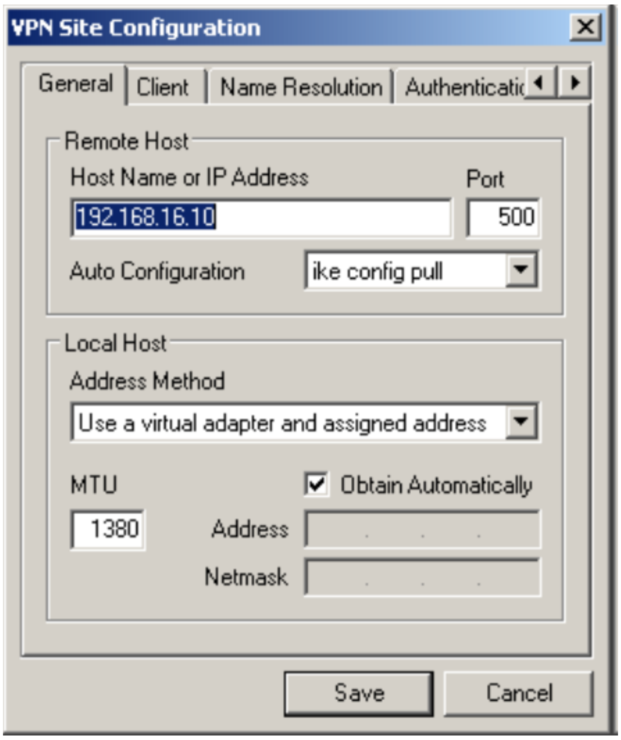
☐ **Include User PIN**
Request PIN during connection, and send with authentication.

☐ **Enable VPN On Demand**
Domain and host names that will establish a VPN

Proxy
Configure the proxy to be used with this VPN connection.
None

Image 282 – IPhone (establishing VPN)

ShrewSoft VPN Client with certificate


VPN Site Configuration
General
Client
Name Resolution
Authenticatic
Save
Cancel

Remote Host

Host Name or IP Address: 192.168.16.10

Port: 500

Auto Configuration: ike config pull

Local Host

Address Method: Use a virtual adapter and assigned address

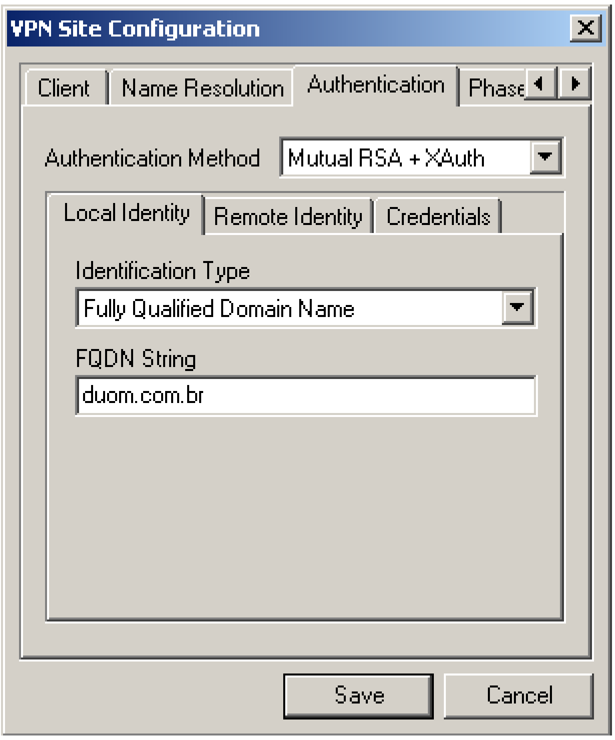
MTU: 1380

☑ Obtain Automatically

Address

Netmask

Image 283 – VPN configuration with certificate.

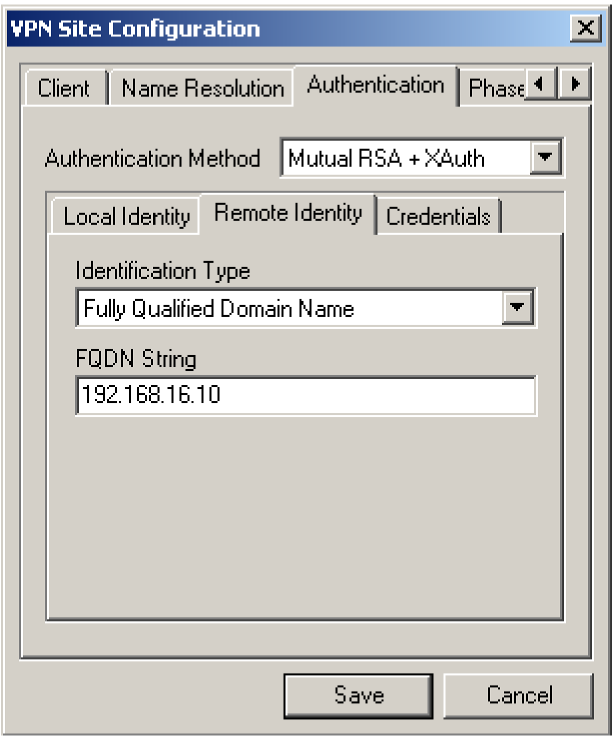

VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Local Identity
Remote Identity
Credentials
Save
Cancel

Authentication Method: Mutual RSA + XAuth

Identification Type: Fully Qualified Domain Name

FQDN String: duom.com.br

Image 284 – VPN configuration (Authentication – Local Identity)

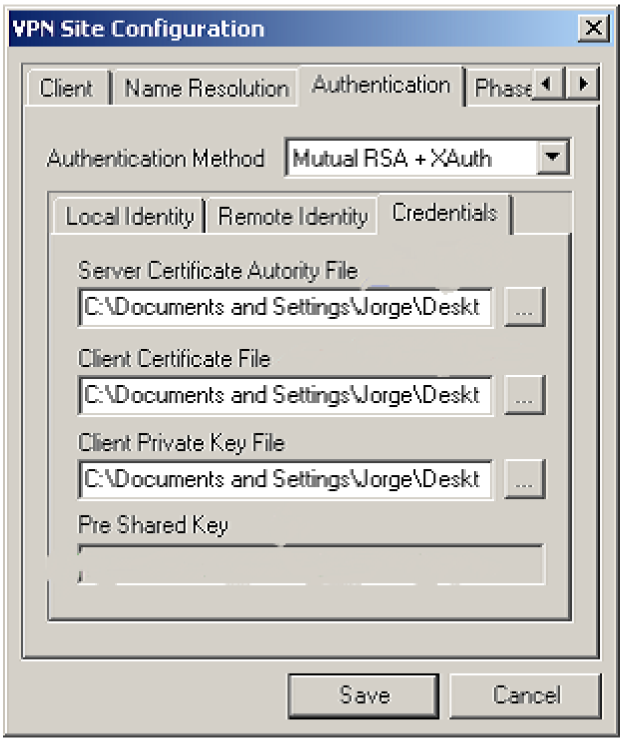

VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Local Identity
Remote Identity
Credentials
Save
Cancel

Authentication Method: Mutual RSA + XAuth

Identification Type: Fully Qualified Domain Name

FQDN String: 192.168.16.10

Image 285 – VPN configuration (Authentication Remote Identity)



VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Local Identity
Remote Identity
Credentials
...
Save
Cancel

Authentication Method: Mutual RSA + XAuth

Server Certificate Autority File: C:\Documents and Settings\Jorge\Deskt

Client Certificate File: C:\Documents and Settings\Jorge\Deskt

Client Private Key File: C:\Documents and Settings\Jorge\Deskt

Pre Shared Key

Image 286 – VPN configuration (Authentication – Authentication Method)

10.6. VPN – SSL

The VPN SSL Portal is from Apple and is very simple to be managed, once all the portal operation and applet details are responsibility of the firewall. The administrator will define which certificate will be used by the firewall and etc.

All of these configurations are available in the *VPN SSL window*, to gain access to it follow the images bellow:

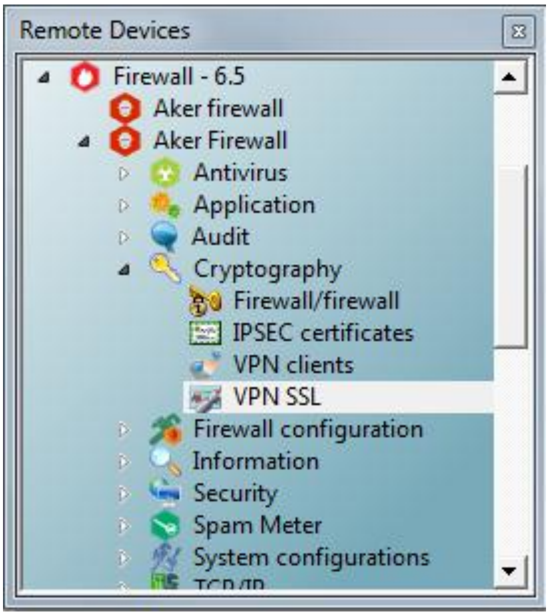
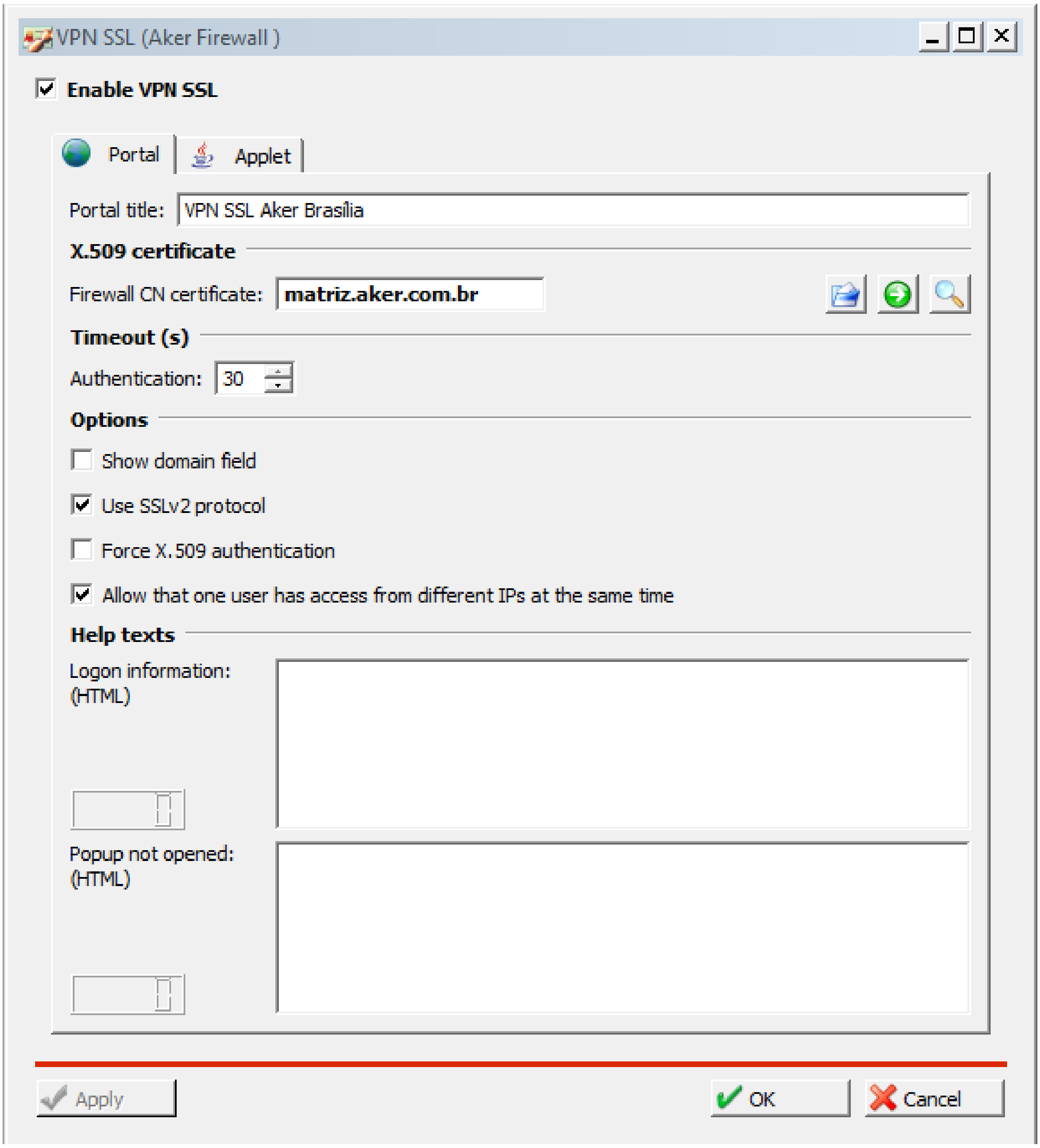

Remote Devices
Firewall - 6.5
Aker firewall
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall/firewall
IPSEC certificates
VPN clients
VPN SSL
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 287 – Access window (VPN SSL)

- Click on the *Cryptography* menu in the main window.
- Choose *VPN SSL*.

When selecting the option *Enable VPN SSL*, the applet and portal configuration will be enabled.

Portal



☑ Enable VPN SSL

Portal title: VPN SSL Aker Brasília

X.509 certificate

Firewall CN certificate: matriz.aker.com.br

Timeout (s)

Authentication: 30

Options

☐ Show domain field

☑ Use SSLv2 protocol

☐ Force X.509 authentication

☑ Allow that one user has access from different IPs at the same time

Help texts

Logon information: (HTML)

Popup not opened: (HTML)

Image 288 – VPN SSL (Portal)

In the web portal, the client authenticate himself in the firewall and as result receives the applet that implements the SSL tunnel.

Portal title: This field informs the portal’s name and it has a maximum limit of 64 characters.

Firewall CN certificate: This field informs the name of the certificate applied to the Firewall.

When clicking on the icon 📂 a *.p12/*.pfx file containing the certificate will be loaded. The icon 🔍 shows a summary of the certificate information and the icon ➔ allows exporting a file with extension *.p12/*.pfx containing a certificate.

Authentication: This field informs the authentication expiration date in the portal, being the maximum time that a session can take to be established, varying from 0 to 30 seconds.

Show domain field: When selected this option allows showing the domain field in the portal login form.

Use SSLv2 protocol: When selected this option chooses using the SSL protocol version 2.

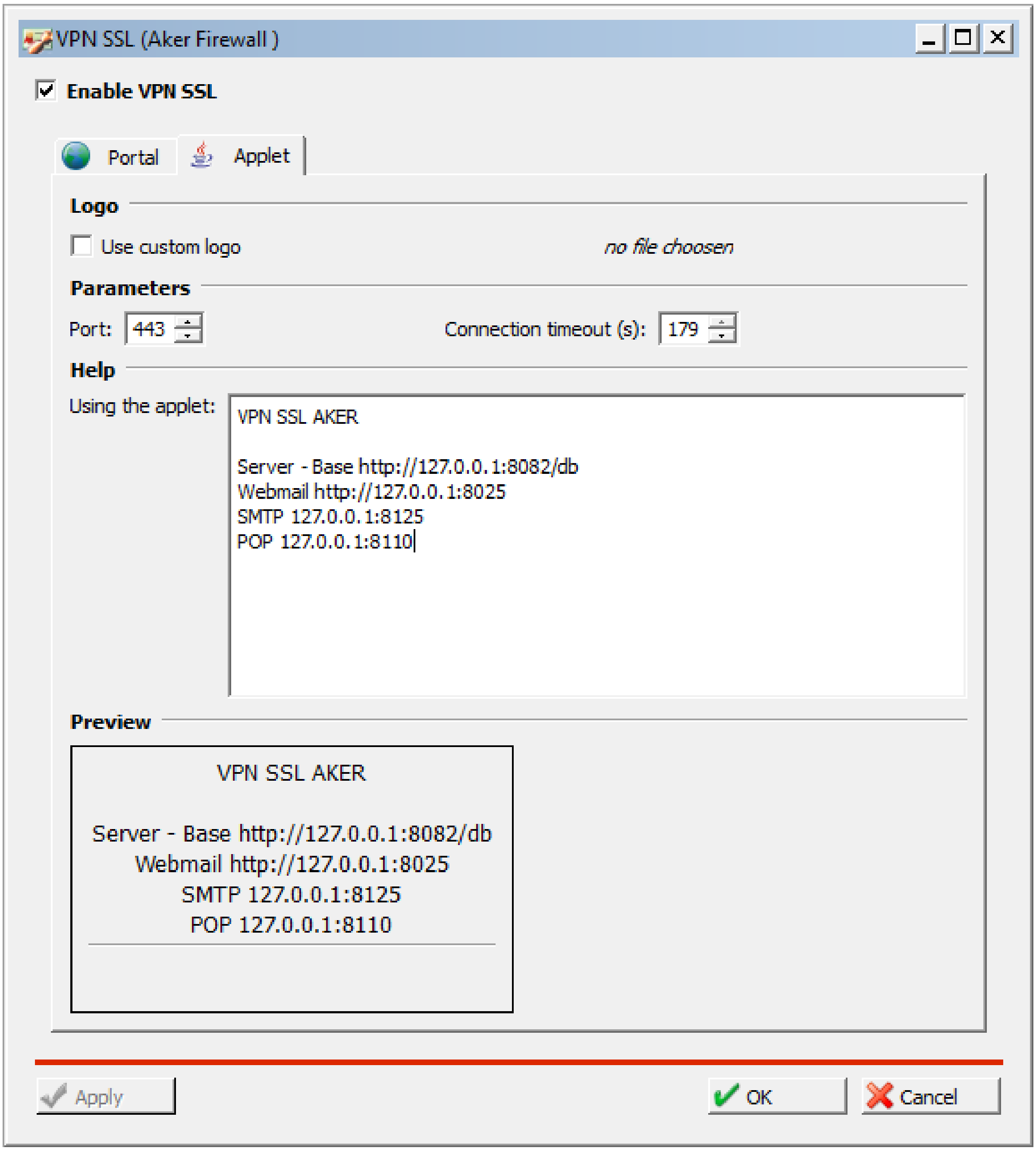
Force x.509 authentication: When selected this option allows forcing a X.509 authentication, because it prevents the user to authenticate himself using any other method which is not through a digital certificate.

Allow that one user has access through different IPs at the same time: This option allows the user log in the portal through one or more different portals.

Logon information: This field allows including the text that will be presented in the portal as basic information about its functioning. It does not have a defined size and can be written using the HTML format.

pop-up not opened: This field is informational. In case applet displays error when loading, this text will be displayed to user as response to error that has occurred.

Applet



VPN SSL (Aker Firewall)
Portal
Applet
Logo
Parameters
Help
Preview
Apply
OK
Cancel

☑ Enable VPN SSL

☐ Use custom logo   *no file choosen*

Port: 443   Connection timeout (s): 179

Using the applet:

```
VPN SSL AKER

Server - Base http://127.0.0.1:8082/db
Webmail http://127.0.0.1:8025
SMTP 127.0.0.1:8125
POP 127.0.0.1:8110
```

Image 289 – VPN SSL (Applet)

Use custom logo: When enabled this option allows the user to present his/her logo in the applet.

Change file: This button allows changing the logo. This button appears when the option *Use custom logo* is selected. ...

Port: This option allows defining the port which the applet will use to connect in the firewall in order to make the SSL tunnel.

Timeout connection: This field informs the time in seconds that the connection can remain without traffic any data in the SSl tunnel. When this time expires the tunnel will be closed.

Using the applet: This field shows general information about applet usage. The text cannot be in HTML format and it does not have a defined size.

Preview: In this area all visual configurations applied to applet can be visualized including Aker and client's title and logo

Client

The client needs the browser and the Java Host installed to gain access, which is performed through URL: https\\ IP of the firewall selected to be accessed.

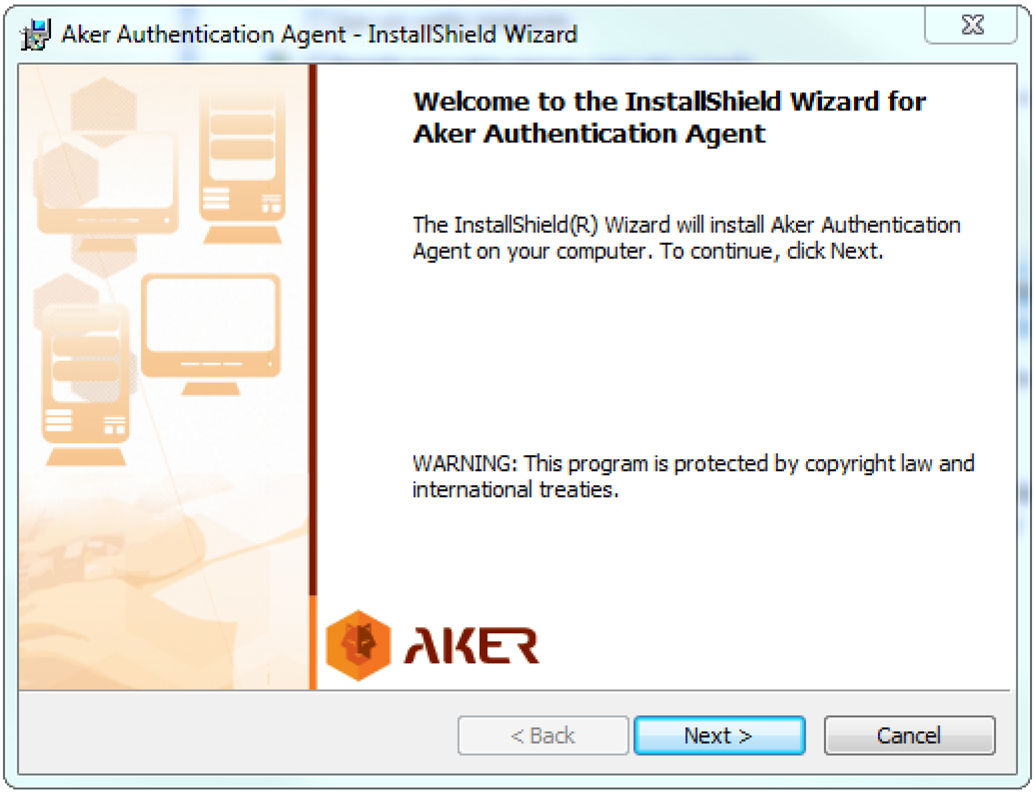
To gain access to this feature is necessary to enable the ***"WEB Filter"*** and check the option ***"force authentication"*** in the ***General*** tab**.**

After user accepts the certificates, an authentication window where user and password will define which access profile and which communication ports will have permission in the VPN will be displayed.

Aker Authentication Agent installation

To perform the installation follow the steps bellow:

- Download Aker Authentication Agent;
- Run the installer and click on **"Next";**
- The License agreement will be displayed in the next window;



Aker Authentication Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for Aker Authentication Agent

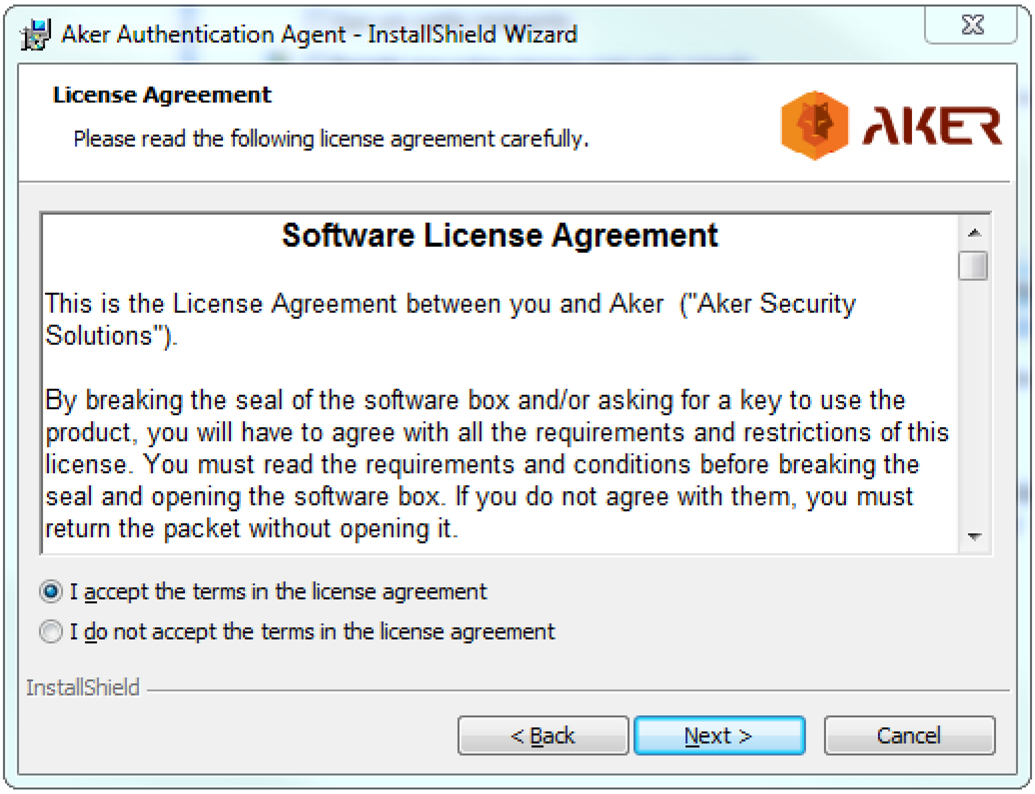
The InstallShield(R) Wizard will install Aker Authentication Agent on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

AKER
< Back
Next >
Cancel

Image 290 – Aker Authentication Agent wizard welcome screen.

- Read the License agreement**;**
- Click on the option **"I accept the terms in the license agreement"**;
- Click on **"Next";**


Aker Authentication Agent - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AKER

Software License Agreement

This is the License Agreement between you and Aker ("Aker Security Solutions").

By breaking the seal of the software box and/or asking for a key to use the product, you will have to agree with all the requirements and restrictions of this license. You must read the requirements and conditions before breaking the seal and opening the software box. If you do not agree with them, you must return the packet without opening it.

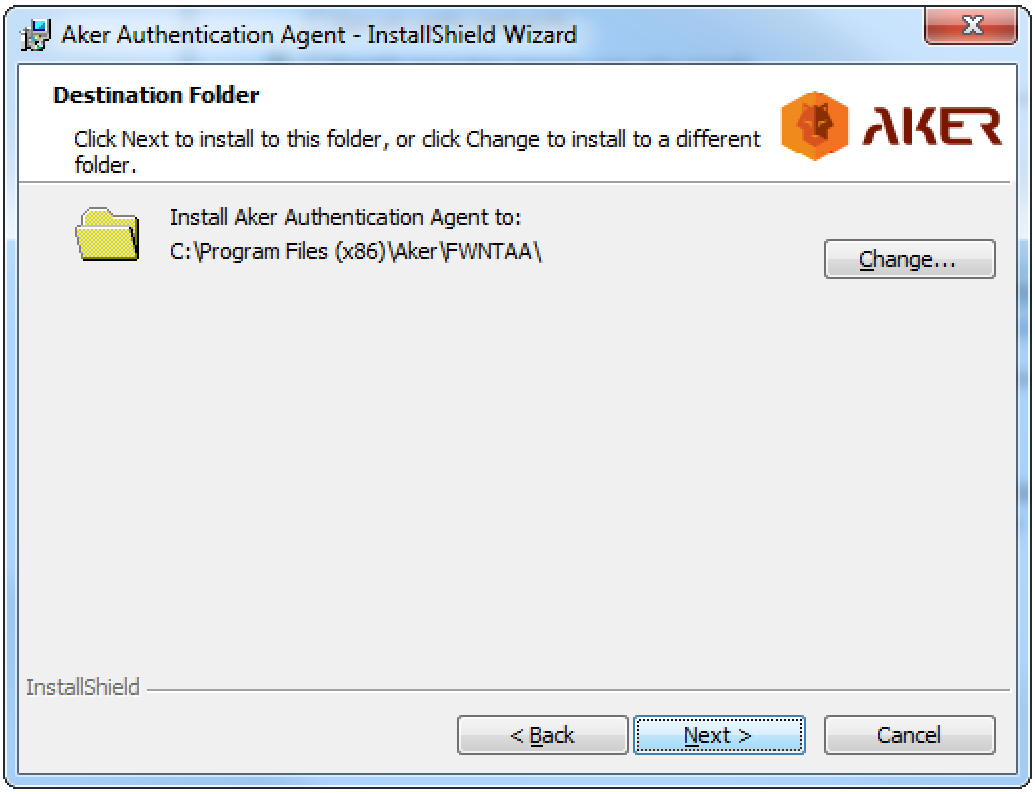
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

InstallShield
< Back
Next >
Cancel

Image 291 – License agreement.

- “Destination folder”; will be displayed
- In case you wish to install the program in a different folder, click on **“Change”**. If you wish install the program in the selected folder click on **“Next”;**



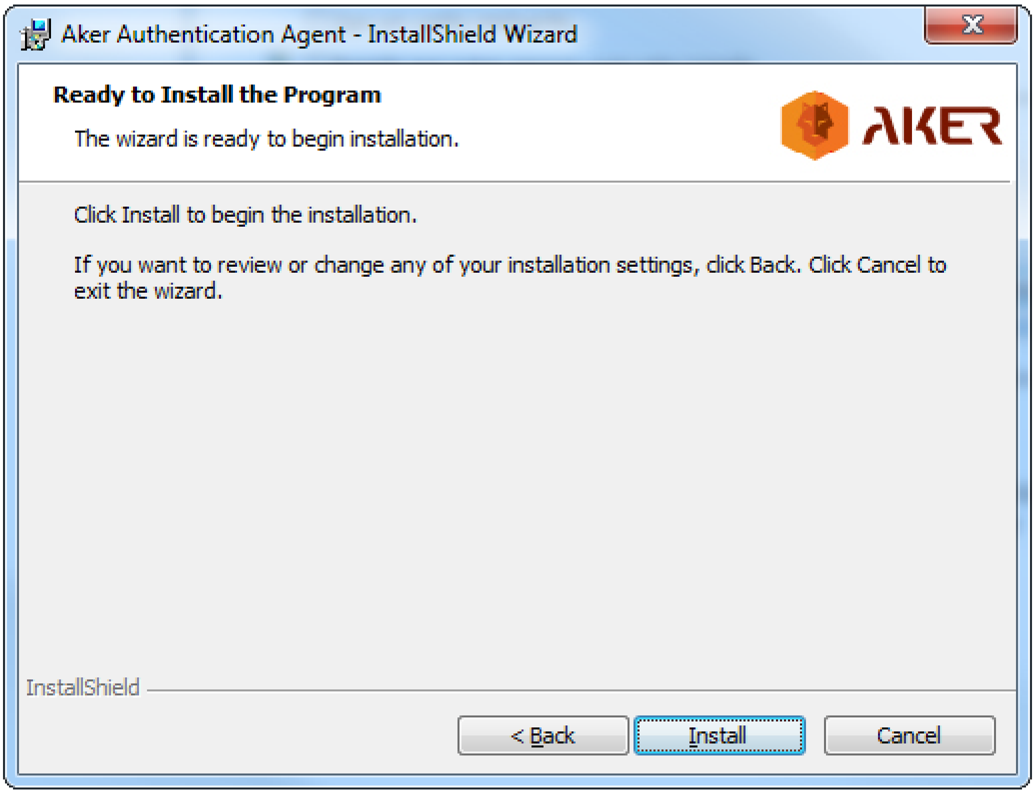
Aker Authentication Agent - InstallShield Wizard
Destination Folder
AKER
Change...
InstallShield
< Back
Next >
Cancel

Click Next to install to this folder, or click Change to install to a different folder.

Install Aker Authentication Agent to:
C:\Program Files (x86)\Aker\FWNTAA\

Image 292 – Destination folder.

- A screen with the following message: **“Ready to install the program”** will be displayed. If all configurations are set, click **“Install”**, if there is a need of making any change click on **“Back”.**



Aker Authentication Agent - InstallShield Wizard

Ready to Install the Program

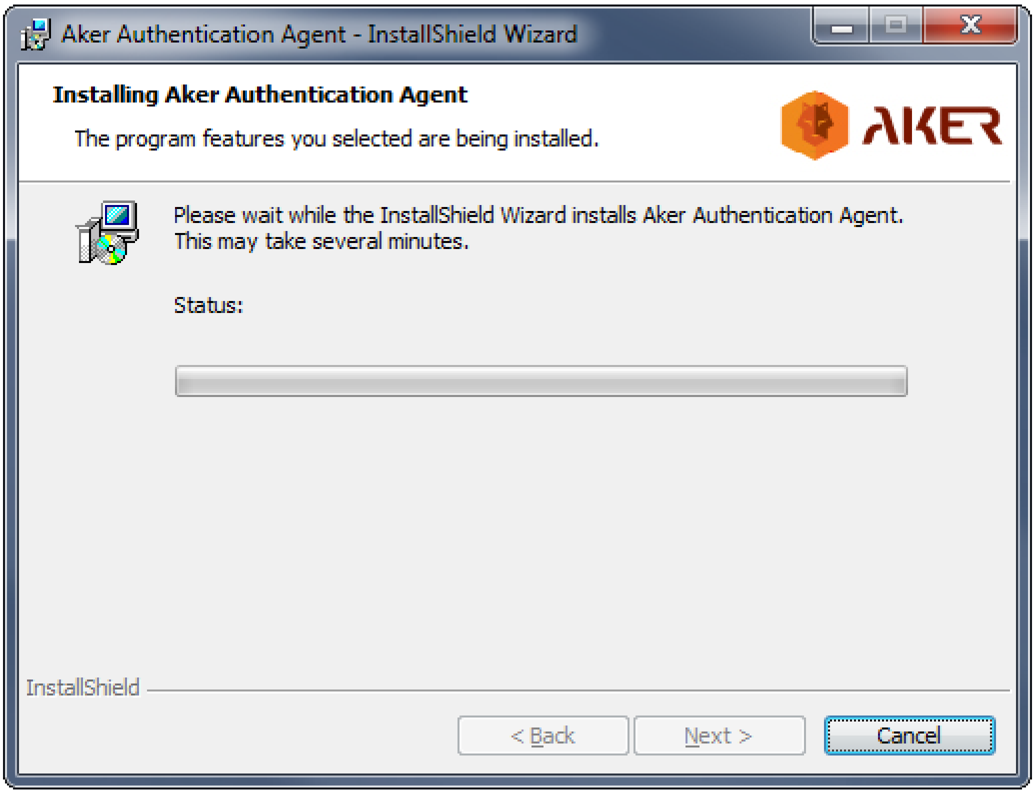
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Image 293 – Installing the program.

- A screen showing the Installation status bar will be displayed, in case you wish to stop the installation click **“Cancel”.**



Aker Authentication Agent - InstallShield Wizard

Installing Aker Authentication Agent

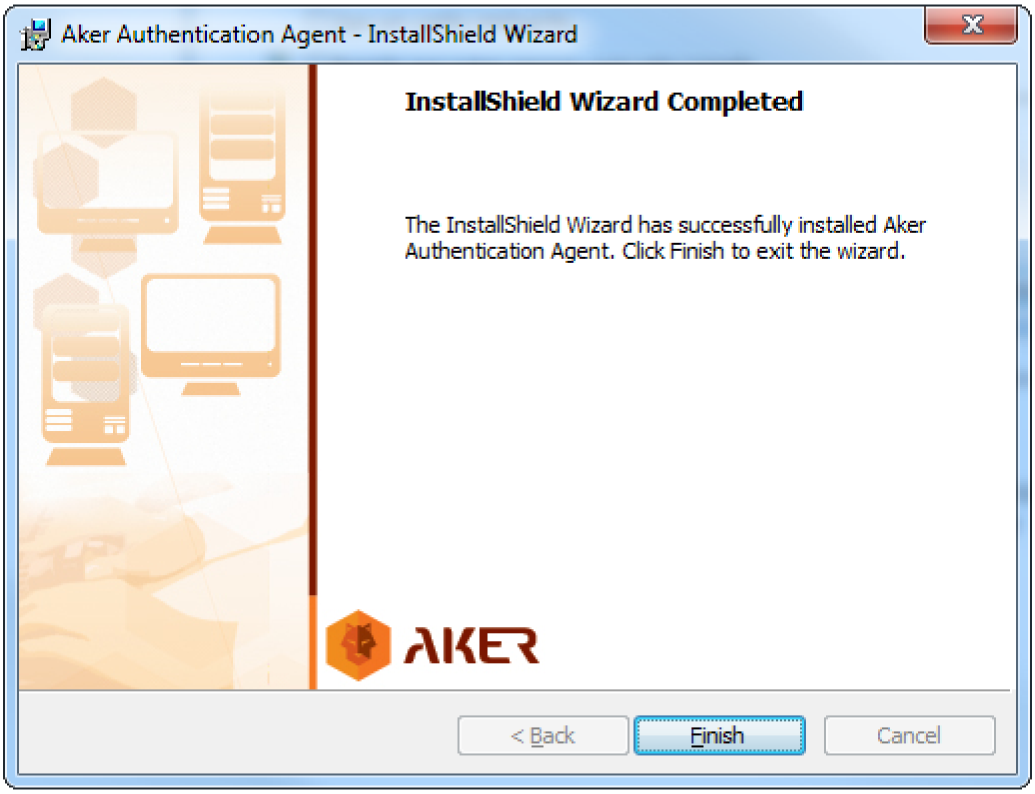
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Aker Authentication Agent. This may take several minutes.

Status:

Image 294 – Installation status bar.

- The installation has been completed.

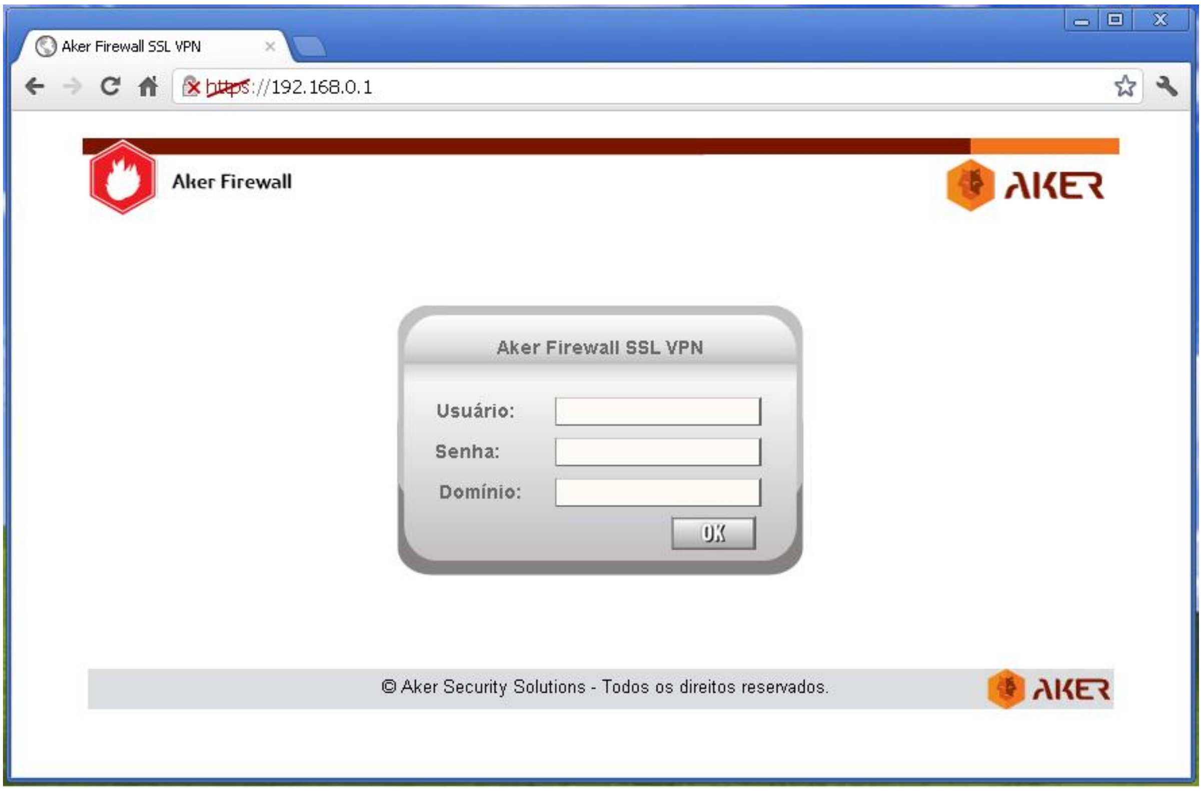


Aker Authentication Agent - InstallShield Wizard
AKER
< Back
Finish
Cancel

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Aker Authentication Agent. Click Finish to exit the wizard.

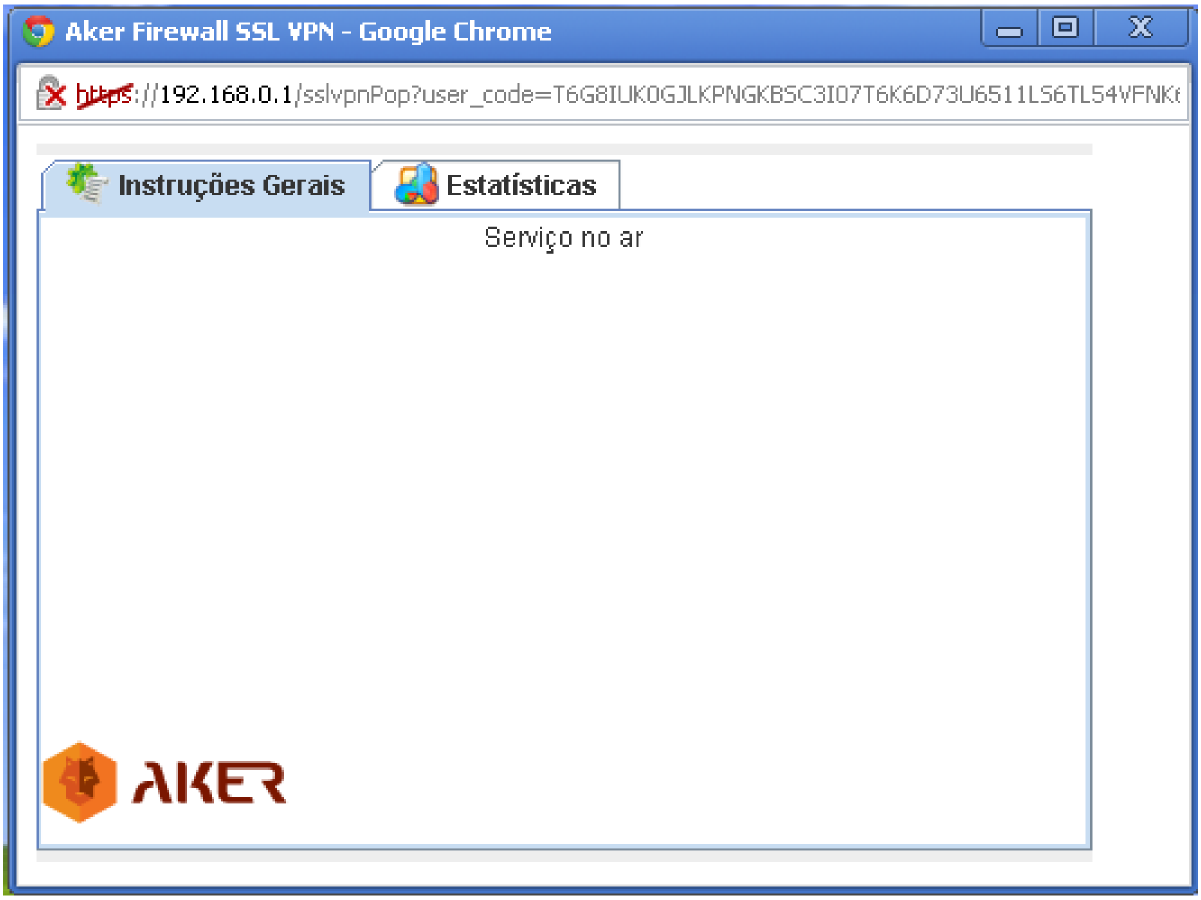
Image 295 –Aker Authentication Agent installation has been completed.



Aker Firewall SSL VPN
https://192.168.0.1
Aker Firewall
Aker Firewall SSL VPN
Usuário:
Senha:
Domínio:
OK
© Aker Security Solutions - Todos os direitos reservados.

Image 296 – Access Profiles (VPN Permission)

After the authentication is performed successfully we shall have the Applet running with the information which has been configured in the Applet session:


Aker Firewall SSL VPN - Google Chrome
~~https~~://192.168.0.1/sslvpnPop?user_code=T6G8IUK0GJLKPNGKBSC3I07T6K6D73U6511LS6TL54VFNK
Instruções Gerais
Estatísticas

Serviço no ar

Image 297 – VPN SSL – General instructions.

The access to services through VPN are performed through the IP:

127.0.0.1:<port>

This communication port is configured in **Firewall Configuration, Profiles in the VPN-SSL (Proxy SSL) tab.**

Configuring the Proxy SSL

11. Configuring Client-Firewall encryption

This chapter shows what is for and how to configure the SSL Proxy in Aker Firewall.

What is a SSL Proxy?

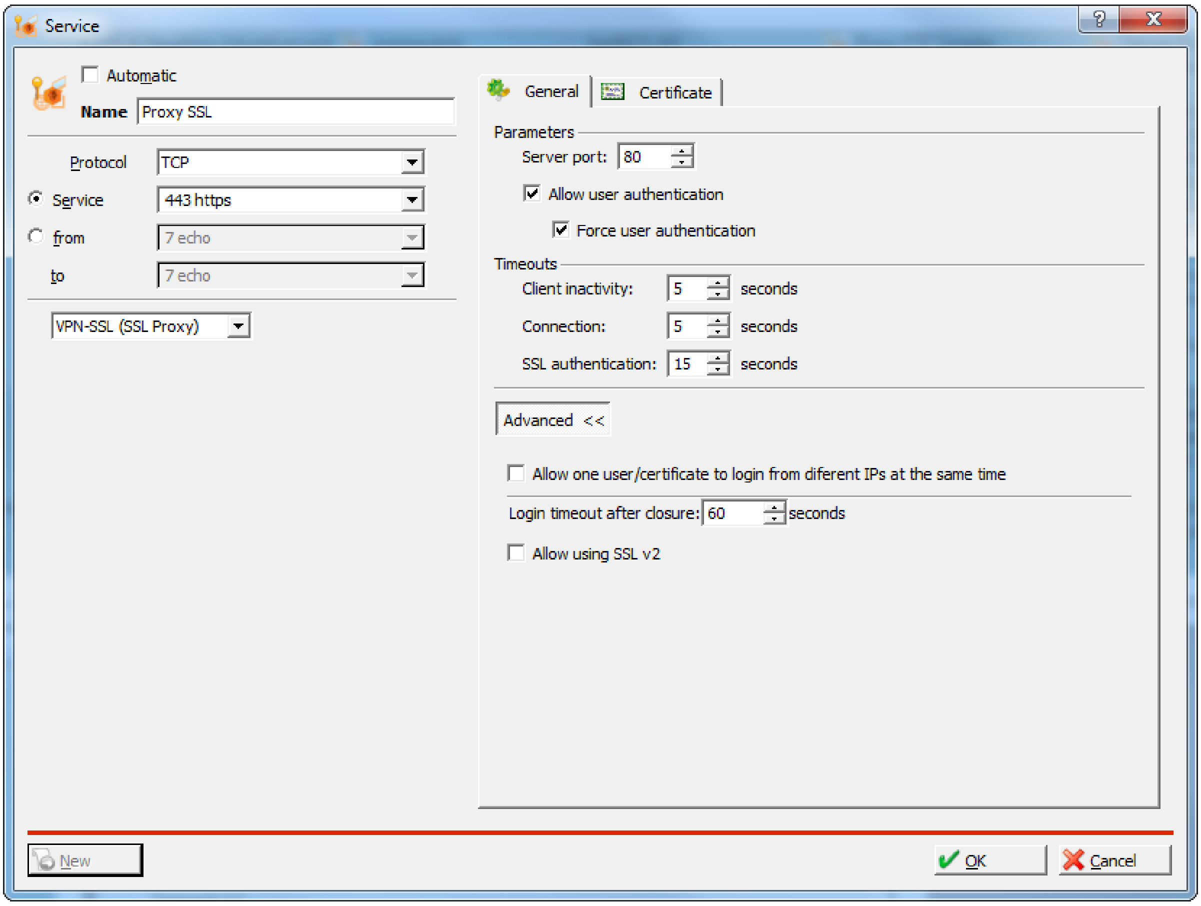
A SSL Proxy is a VPN client-firewall, it is made through the SSL protocol and its main characteristic is the native support to these protocols which is present in several applications such as browsers, e-mail readers, terminal emulator, etc. Due to the native support these application, it is not necessary the installation of any client to VPN establishment.

Its functioning is simple; from a side the client connects to the firewall through the SSl protocol, authenticating himself through X.509 certificates and the firewall connects to the internal firewall. This way the client sees a SSL connection with the server.

Using a SSL Proxy

To use the SSL Proxy in a communication follow the steps bellow:

- Create a service that will be intercepted by the SSL Proxy and edit the context parameters selected to be used by this service (for more information see the chapter titled **Registering Entities**).
- Add a SSL profile filtering rule allowing the use of the created service in the step above, for the desired network or hosts (for more information see the chapter titled **Configuring SSL Proxy rules**).



☐ Automatic
Name Proxy SSL

Protocol: TCP
● Service: 443 https
○ from: 7 echo
to: 7 echo

VPN-SSL (SSL Proxy)

Parameters
Server port: 80
☑ Allow user authentication
☑ Force user authentication

Timeouts
Client inactivity: 5 seconds
Connection: 5 seconds
SSL authentication: 15 seconds

Advanced <<

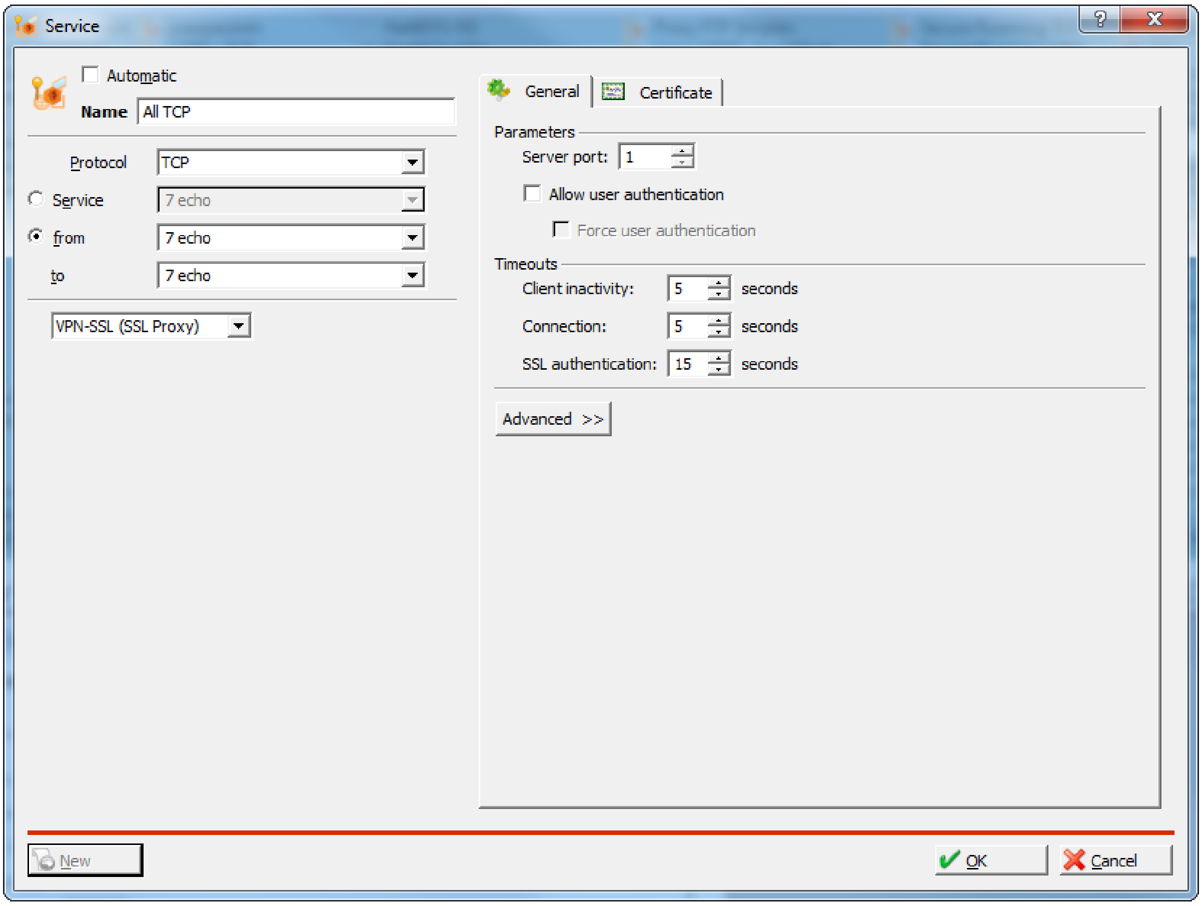
☐ Allow one user/certificate to login from diferent IPs at the same time
Login timeout after closure: 60 seconds
☐ Allow using SSL v2

Image 298 – VPN SSL – General instructions.

11.1. Editing the SSL context parameters

The SSL context properties window will be displayed when the SSL proxy option is selected. Through the SSL context is possible defining the SSL proxy behavior when it deals with the service in question.

SSL context properties window



Service

☐ Automatic

Name All TCP

Protocol TCP

○ Service 7 echo

● from 7 echo

to 7 echo

VPN-SSL (SSL Proxy)

Parameters

Server port: 1

☐ Allow user authentication

☐ Force user authentication

Timeouts

Client inactivity: 5 seconds

Connection: 5 seconds

SSL authentication: 15 seconds

Image 299 – SSL context parameters edition.

In the property window all the context parameters assigned to a specific service are configured. It consists of two distinct tabs: the first one allows configuring the parameters and the second allows the definition of the certificate that will be presented to the client in the VPN establishment.

General Tab

Server Port: This field indicates the port that the server will be waiting to receive the connection.

Allow user authentication: If checked this field indicates that the users can authenticate themselves in the SSL Proxies establishment. In case it is unchecked, only anonymous sessions will be authorized.

Force user authentication: If this field is checked, SSL Proxy sessions which the user has not presented a valid X.509 certificate will not be authorized.

Client inactivity: This field indicates the maximum time in seconds that the firewall will keep the SSL Proxy session active (since it has already been established) without the receiving of data from the client.

Connection: This field indicates the maximum time in seconds that the firewall will wait for the connection establishment with the server.

SSL authentication: This field indicates the maximum time in seconds that the firewall will wait for the client performs a successful SSL authentication.

Advanced: This button grants access to configuration parameters that are not usually used.

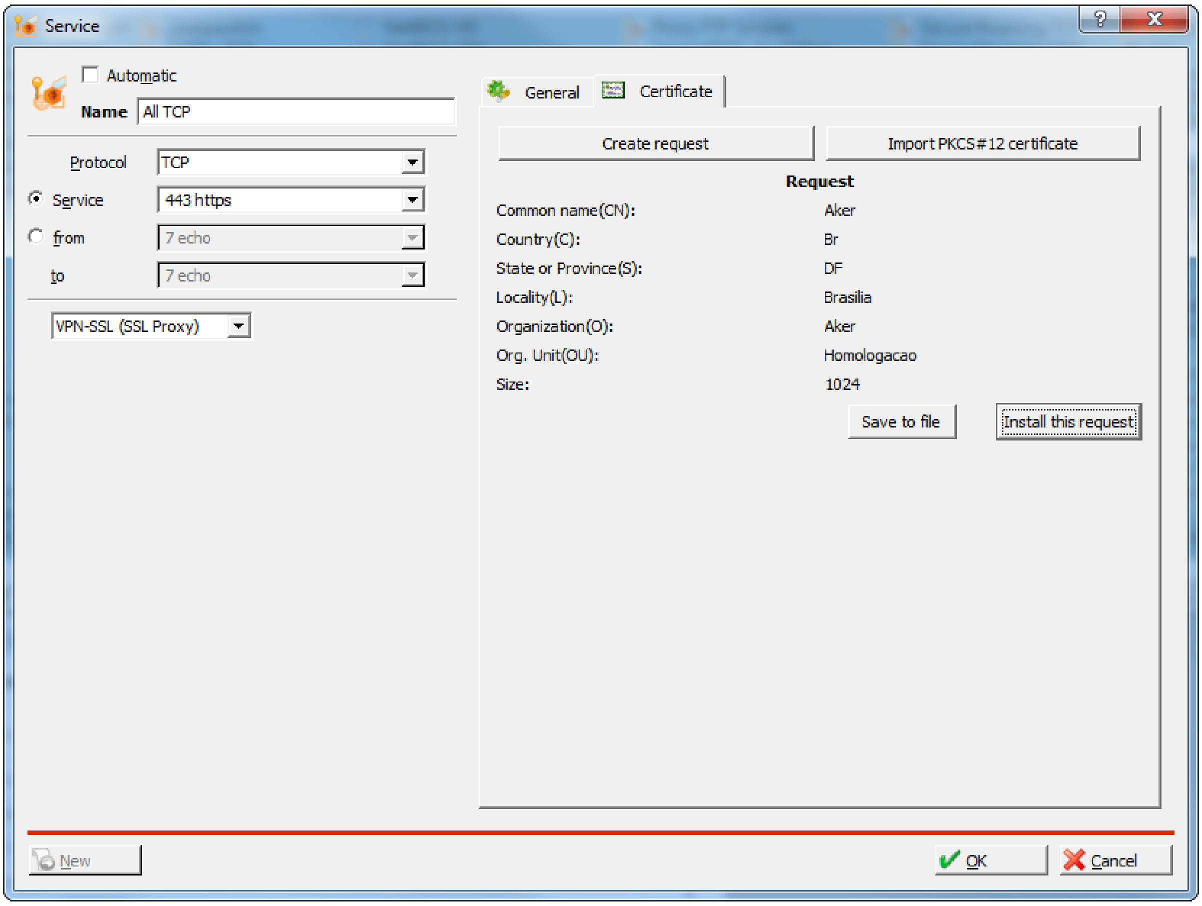
Allow one user/certificate to login from different IPS at the same time: If checked this field allows a user to establish simultaneous connection from different hosts. In case it is unchecked, if a user already has a session in one hosts, opening attempts from other hosts will be refused.

Login timeout after closure: As there is no concept of session in a SSL Proxy, is necessary that the proxy simulates a session keeping a user logged in for a while after the last connection closes, in case it is necessary stopping the same user from accessing different hosts simultaneously. This field specifies the time in seconds that the firewall must to consider a user as logged after the last connection is closed.

Allow using SSL v2: This field indicates whether the firewall shall or not accept a SSL connection using the 2nd version of this protocol.

SSL protocol has few security problems and the use of it is not recommended, unless it is strictly necessary.

Certificate Tab



☐ Automatic

Name All TCP

Protocol TCP

● Service 443 https

○ from 7 echo

to 7 echo

VPN-SSL (SSL Proxy)

Request

Common name(CN):	Aker
Country(C):	Br
State or Province(S):	DF
Locality(L):	Brasilia
Organization(O):	Aker
Org. Unit(OU):	Homologacao
Size:	1024

Image 300 – View owner's certificate – X.509.

This tab is used to specify the X.509 certificate which will be presented to the client when he is attempting to establish a SSL Proxy. It is possible to create a request which will be sent afterward to be signed by a CA or import a certificate X.509 that is already assigned, in PKCS#12.

Create request:

This button allows creating a request which will be sent to a CA afterward in order to be signed. When clicked this option shows the new certificate fields that need to be filled in.

After the fields are filled in, click on **Ok** then the window will be changed and a newly created request will be shown. You have two options to manage the request; one of them is ***Save*** that saves the request in a file in order to send it to a CA to get signed. The button ***Install this request*** allows you to import a certificate already signed by CA.

Import PKCS#12 certificate:

This button allows you to import a X.509 certificate.

11.2. Configuring Proxy SSL rules

After the definition of one or more SSL contexts, presented in the previous topic, it is necessary to configure the users' access profiles in order to define what services they can access through the VPN SSL session. This configuration is located in the SSL tab, inside each access profile.

For more information about registering rules, see the topic **Registering access profiles.**

Integration of the Firewall modules

12. Integration of Firewall modules

In this chapter, the relationship of the three large Aker Firewall modules will be displayed: the packet filter, the network address translator, the encryption, and authentication module. The path through which the packets go from the moment they are received by the Firewall until the moment they are accepted or rejected will also be displayed.

12.1. The flow of packets on Aker Firewall

In the previous chapters of this manual, the three large Aker Firewall modules were displayed separately and all the details pertinent to the configuration of each one. Now, it will be displayed how a packet goes through them and which changes it can suffer in each one of them.

Basically, there are two different flows: one for packets that are generated in the Intranet and have an external host as destination (inside-outside flow) or packets that are generated in the external network and have a host on the Intranet as destination (outside-inside flow).

The flow from the inside out

When any packet from the Intranet reaches the firewall, it goes through the modules in the following order: assembler module, packet filter, network address translator and encryption module.

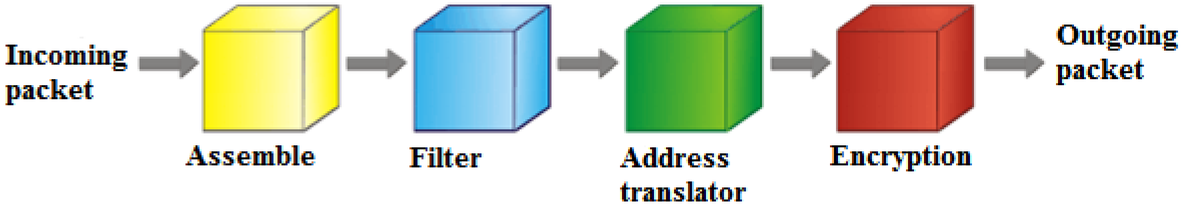


Image 301 – Intranet packet flow when reaching the firewall.

The assembler module

The assembler module is responsible for storing all fragments of the received IP packets until they can be reassembled and converted into a complete packet. This packet will be passed to the other modules.

The packet filter

The packet filter has the basic function of validating a packet in accordance with the rules defined by the administrator, and its stateful table, and deciding whether it should be allowed to pass through the firewall. If it decides that the packet can pass, it will be passed to the other modules, otherwise, it will be discarded and the flow will end.

The network address translator

The network address translator receives an authorized packet and verifies, according to its configuration, if it should have the source address translated. In case of positive answer, it translates the packet otherwise, the packet will suffer no other alterations.

Afterwards, the packet will be passed to the encryption module.

The encryption module

The encryption module receives a valid packet, with translated addresses, and decides, based on its configuration, if this packet should be encrypted or authenticated before being sent to the destination. In case of positive answer, the packet will be authenticated, encrypted, and some specific headers will be added to it.

Afterwards, the packet will be sent through the network.

The flow from the outside in

When any packet coming from the external network, in direction towards the Intranet, reaches the firewall, it goes through the modules in the following order: assembler module, decryption module, network address translator and packet filter.

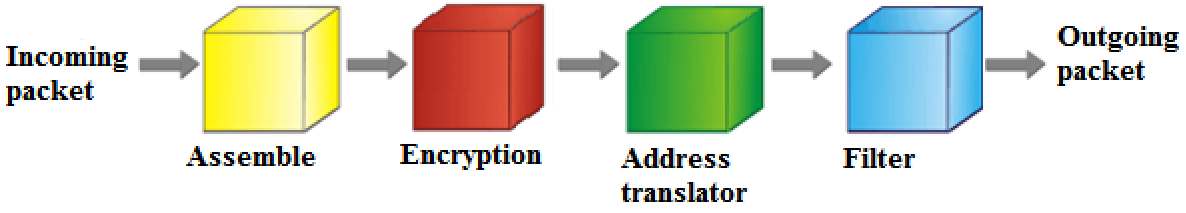


Image 302 – External network packet flow towards the Intranet.

The assembler module

The assembler module is responsible for storing all fragments of the received IP packets until they can be reassembled and converted into a complete packet. This packet will be then passed to the other modules.

The decryption module

The decryption module removes the headers added by the encryption module, verifying the packet authentication signature and decrypting it. In case either the authentication or the decryption presents an error, the packet will be discarded.

The other function of this module is make sure that all the packets that arrive from a network which there is a secure channel, come encrypted. In case a packet comes from a network which there is an encryption or authentication channel and this packet is not either authenticated nor encrypted, it will be discarded.

If the packet has been validated successfully, it will be passed to the network address translator.

The network address translator

The network address translator receives a packet and checks if the destination address of this packet is one of the virtual IP addresses. In case of positive answer, this address is translated to a real address.

Afterwards, the packet will be passed to the packet filter.

The packet filter

The packet filter is the last module of the *outside-in* flow. It has the basic function of validating the received packet according to the rules defined by the administrator, and its stateful table, and deciding whether it should be allowed to pass through the firewall. If it decides that the packet can pass, it will be sent to the destination host; otherwise, it will be discarded.

12.2. Integrating the filter with the address translation

When configuring filtering rules to be used with hosts whose addresses will be translated, the following doubt arises: should the real hosts' addresses be used or the virtual ones?

This question can be easily answered while analyzing the packet flow:

- In the *inside out* flow, the packets go through the filter first and then have their addresses translated (if it is the case), that means, the filter receives the real addresses from the hosts.
- In the *outside in* flow, the packets go through the network addresses translator first, which translates the destination addresses of the virtual IP addresses into the real ones. After this, the packets are sent to the packet filter, this means, the packet filter receives the packets with the real addresses again.

In both cases, the filter is not aware of the virtual addresses existence.

When filtering rules are created, the network addresses translation must be ignored. The rules must be configured as if the source and destination hosts were communicating directly, without using any kind of addresses translation.

12.3. Integrating the filter with the network address translation

In the previous section, we have displayed how to configure the filtering rules to hosts whose addresses would be translated. The conclusion was that you should work only with the real addresses, ignoring the address translation. Now, one more question arises: when secure channels are configured to hosts that will go through the network address translation, should the real addresses of these hosts be used or the virtual ones?

In order to answer this question, the packet flow should be analyzed again:

In the *inside out* flow, the packets go through the filter first, have their addresses translated (if it is the case) and, at last, they are passed to the encryption module. Due to this fact, the encryption module receives the packets as if they were originated in the virtual addresses.

In the *outside in* flow, the packets go through the decryption module and are decrypted (if it is the case). Then, they are sent to the network addresses translator, which translates the destination addresses of the virtual IP addresses into real addresses, and, at last, they are sent to the packet filter. The decryption module receives the packets before they have had their addresses translated and, consequently, with the virtual addresses.

In both cases, the encryption and decryption modules receive the packets as if they had their origin or destination in the virtual IP addresses, what leads us to the following statement:

When secure channels are created, you should pay attention to the network addresses translation. The source and destination addresses must be set as if the channel had the virtual IP addresses as its origin or destination.

Configuring the Security

13. Configuring the security

This chapter shows how to configure the protection against attacks on Aker Firewall security module.

13.1. Protection against SYN Flood

What is a SYN Flood attack?

SYN Flood is one of the most popular denial of service attacks. The purpose of these attacks is to deny the functioning of a host or a specific service. In case of the SYN flood, it is possible to make any TCP based service unusable.

In order to understand this attack, it is first necessary to understand the functioning of the TCP protocol related to connection establishment.

The TCP protocol uses a 3-way handshake to establish a connection:

1. The client host sends a packet to the server with a special flag called the SYN flag. This flag indicates that the client wants to establish a connection.
2. The server responds with a packet containing both the SYN and ACK flags, which means that the server has accepted the request for the connection and that it is waiting for a confirmation from the client in order to have the connection established.
3. The client, right after receiving the packet with the SYN and ACK, responds with a packet containing only the ACK flag, which indicates to the server that the connection has been successfully established.

All connection requests received by a server are stored in a special queue which has a predetermined size, dependent on the operating system. They are kept stored until the server is informed by the client that the connection has been established. In case the server receives a connection request packet and the pending connections queue is full, this packet is discarded.

Basically, the attack consists of sending a large number of packets of connection request to a specific server. These packets are sent with a source address forged to an inexistent host (reserved addresses described in the chapter about the network address translation are often used in this circumstance). The server, right after receiving these packets, sends a response packet and waits for a confirmation from the client host. As the source address of the packets is false, this confirmation will never reach the server.

What happens is that during a specific moment, the server pending connections queue is found completely full. From this point on, all the requests for connections establishment are discarded, and the service is invalidated. Such invalidation persists for few seconds, for the server, when discovering that the confirmation is taking too long, removes the pending connection from the queue. However, if the attacker keeps sending packets continuously, the service will be kept invalidated for as long as he wishes.

Not all hosts are vulnerable to SYN Flood attacks. Newer implementations of the TCP protocol have mechanisms to cancel out these types of attacks.

How does the Aker Firewall SYN Flood protection work?

Aker Firewall has a mechanism whose purpose is to avoid SYN Flood attacks. Its functioning is based on the following steps:

1. When a connection request packet (packet with the SYN flag, described in the previous topic) is sent to a server to be protected, the firewall registers it in a table and allows the packet to pass (evidently, the packet will only be allowed to pass if this has been authorized by the filtering rules configured by the administrator. For further details, refer to the chapter **The Stateful Filter**).
2. When the server response arrives informing that the connection has been accepted (packet with the SYN and ACK flags), the firewall will immediately send a packet to the server confirming the connection, and it will also allow the response packet to pass towards the client. From this point on, an internal clock will be activated in the firewall. This clock will mark the time during which the confirmation packet from the client must arrive.
3. If the connection request is a regular one, within a period of time shorter than the maximum allowed, the client will respond with a packet confirming the establishment of the connection. This packet will make the firewall validate the connection request and shut down the internal clock.
4. In case the client does not respond within the maximum time allowed, the firewall will send a special packet to the server which will drop the connection.

With all these procedures, the firewall prevents the pending connection queue in the server to overfill. This is possible since all the pending connections will be established as soon as the response packets reach the firewall. The SYN flood attack will not be effective.

It is important to emphasize that the functioning of this protection is based on the timeout for the clients' confirmation packets. If the timeout is too short, valid connections may be refused. If the timeout is too long, the server, in the case of an attack, it will keep a large number of established connections, which may cause even more serious problems.

13.2. Using the Remote Interface for protection against SYN Flood

To gain access to the SYN flood protection against attacks window, follow the steps bellow:

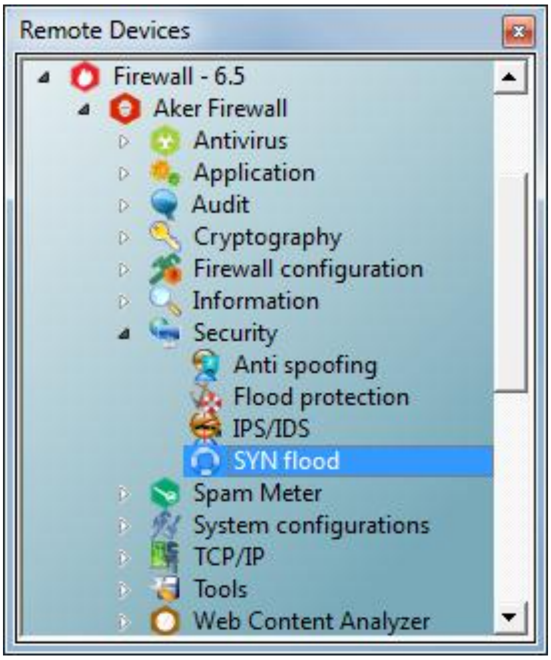
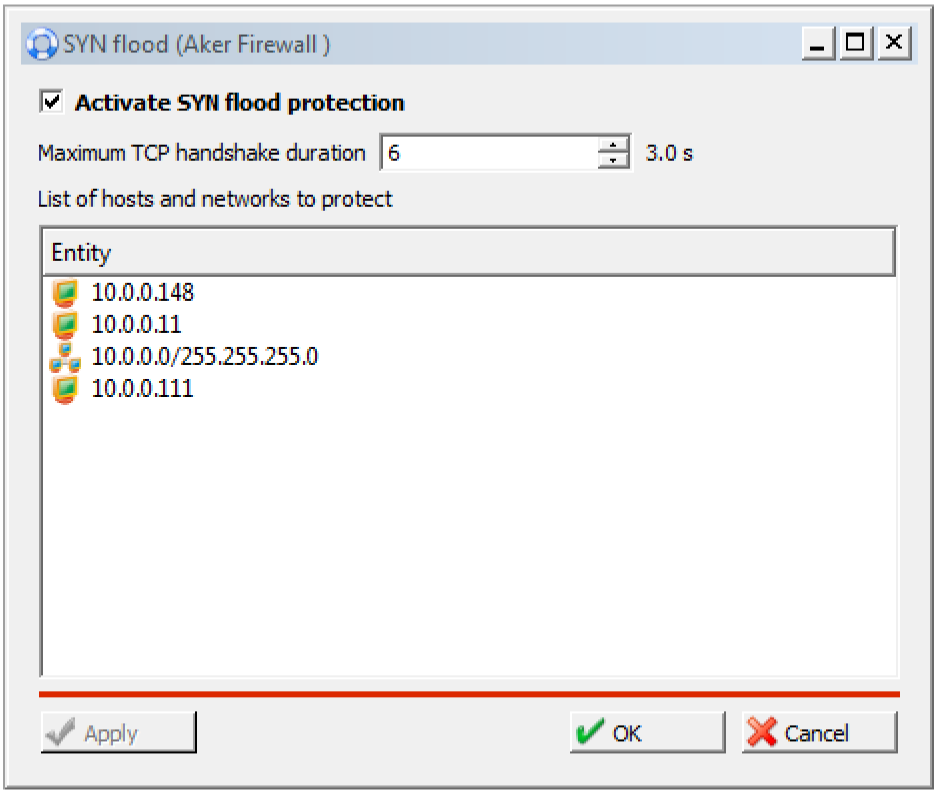

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Anti spoofing
Flood protection
IPS/IDS
SYN flood
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 303 – SYN Flood window.

- Click on the *Security menu* in the firewall window you wish to administrate.
- Choose *SYN Flood.*

SYN flood configuration window



SYN flood (Aker Firewall)

☑ Activate SYN flood protection

Maximum TCP handshake duration 6 3.0 s

List of hosts and networks to protect

Entity
10.0.0.148
10.0.0.11
10.0.0.0/255.255.255.0
10.0.0.111

Figura 304 – SYN Flood – Ativação de proteção SYN Flood.

- The **OK** button updates configuration parameters and closes the window
- The **Cancel** button discards all changes and closes the window.
- The **Apply** button saves all changes to the firewall and keeps the window opened.

SYN flood fields meaning:

Activate SYN flood protection: This option must be checked to activate the protection against SYN Flood, and unchecked to deactivate it (When SYN Flood protection is disabled, old configurations are kept stored but cannot be modified).

Maximum TCP handshake duration: Defines the maximum time period, in 500ms units, a firewall will wait for a client connection confirmation. If this time is reached, a packet will be sent to the server host, dropping the connection.

The ideal value for this field may vary for each installation. However, values from 3 to 10 are suggested, corresponding to time periods between 1.5 and 5 seconds.

List of hosts and networks to protect

This list includes the hosts, networks or sets that will be protected by the firewall.

To add a new entity to the protection list, do one of the following:

- Drag and drop an entity from the hosts, networks or set branches, in the Entities window, straight to the list.
- Right-click on the list of hosts and network to protect to open the context-sensitive menu. Select **Add Entities**. Click on the entity to be added. Click **Add**.

To delete an entity from the list, select it and press delete on your keyboard, or right-click on it, and choose the **Delete** option in the context-sensitive menu.

All TCP servers, with service that can be used by external clients, should be included in the list of entities to be protected. The firewall address should not be added to this list, since FreeBSD and Linux operating systems are not susceptible to SYN Flood attacks.

13.3. Flood Protection

What is a Flood attack?

Flood attacks are characterized by the high number of open and established connections to web, ftp, and smtp, among other servers, from Internet hosts that were invaded and are being controlled and used to spread Denial of Service (DoS) attacks to other hosts.

The protection is also useful to avoid service overuse (download sites, for example), as well as to prevent more serious damages caused by virus, such as NIMDA, which caused that each infected host opened hundreds of connections simultaneously.

How does Aker Firewall Flood Protection work?

Aker Firewall has a mechanism to frustrate flood attacks. Its operation is based on limiting the number of connections that may be simultaneously opened from a same host, to a protected entity.

The firewall administrator must estimate this limit according to daily operation pattern of each server or network being protected.

13.4. Using the Remote Interface for Flood protection

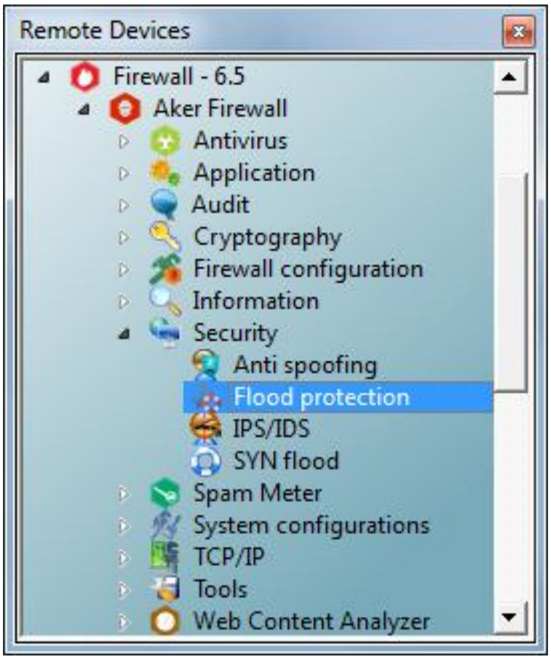
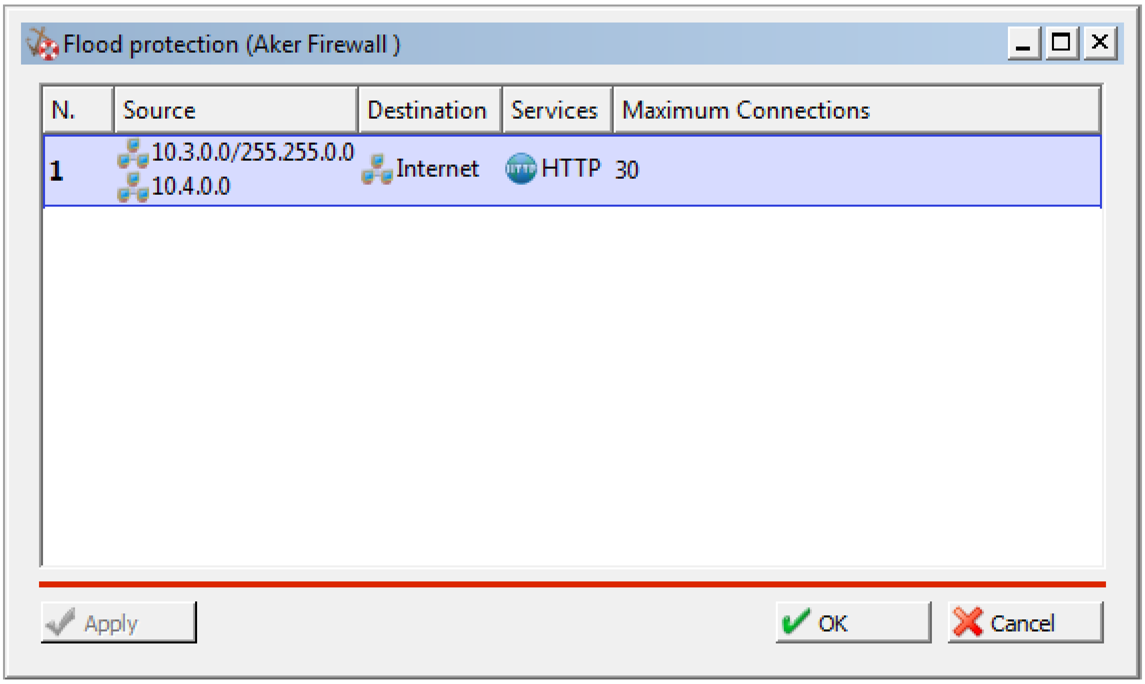

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Anti spoofing
Flood protection
IPS/IDS
SYN flood
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 305 – Access Window: Flood protection.

- Click on the *Security* menu in the Firewall window you want to manage
- Choose *Flood Protection*

Flood Protection



N.	Source	Destination	Services	Maximum Connections
1	10.3.0.0/255.255.0.0 10.4.0.0	Internet	HTTP	30

Image 306 – Flood protection (Configuration)

- The **OK** button updates configuration parameters and closes the window.
- **The Cancel button** discards all change and closes the window.
- **Apply button** saves all changes to the firewall and keeps the window open.

Field meaning:

Number: Corresponds to the Protection Flood rule number.

Source: A network or host that can be the source of DDoS attacks (usually the Internet)

Destination: Hosts or networks that will be protected.

Services: Service that will be protected. More than one entity may be included in this field.

Maximum Connections: Numeric field where you select the maximum number of simultaneous connections an entity can hold, from the same source.

13.5. Anti-Spoofing Security

What is a Spoofing?

IP spoofing involves the supply of false information about a person, or about a host identity, to obtain non-authorized access to systems and/or to the services they provide. Spoofing interferes in the way a client and a server establish a connection. Despite the fact that spoofing is possible with several protocols, the most known of the spoofing attacks is the IP spoofing.

The first step in a spoofing attack is the identification of two destination hosts, which we will call A and B. In most cases, one host (A) will have a trusting relationship with the other (B). It is indeed this relationship that the spoofing attack will try to exploit. Once the destination systems (A and B) have been identified, the attacker will try to establish a connection with B, in such a way that B believes it has a connection coming from A. The real connection request is from the attacker's host, which we will call X. This spoofing is done with X creating and sending a false message (created on X, but with A's source address) requesting a connection with B. When receives this message, B responds generating a similar message, recognizing the request, and establishing sequence code numbers.

Under usual circumstances, this message generated by B would be combined with a third message recognizing the sequence issued by B and sent to the client host. Thus, the handshake would be completed, and the connection could go on. However, since B believes it is communicating with A, B sends its response to A, and not to X. Therefore, to continue acting like A, X will have to respond to B, as if it were A, without knowing the sequence numbers generated by B. Therefore, to successfully represent A, X must guess precisely the sequence numbers B will use to confirm the connection. In certain situations, this is much easier than we can imagine.

Furthermore, besides guessing the sequence number, the intruder X must also ensure that the initial response message from B never gets to A. If A were to receive such message, it would deny to B having requested the connection, and the spoofing attack would fail. To achieve its objective, i.e., to block B-to-A messages, the attacker X usually sends several connection request packets to A, to exhaust its capacity to receive requests, thus preventing it from responding to B. This technique is known as "port violation". When this operation comes to an end, the invader will be able to conclude the fake connection.

IP spoofing, as described above, is a clumsy and tedious strategy. However, a recent analysis revealed the existence of tools capable of executing a spoofing attack in less than 20 seconds. IP spoofing is a dangerous threat, but luckily, it is relatively easy to create protection mechanisms against it. The best defense against spoofing is to configure routers to reject any packet, which alleged source is from an

Intranet. This simple precaution will prevent external hosts to take advantage of reliable relationships within Intranets.

How does Aker Firewall Spoofing Protection work?

Aker Firewall has a mechanism to frustrate Spoofing attacks. It is based on registering firewall-protected networks i.e., networks behind each firewall network interface.

Only packets from registered entities will be accepted in the Intranets. From the external networks, only packets which originating IP addresses do not match any Intranet addresses.

The firewall administrator must evaluate these networks, define corresponding entities, and use the Remote Interface to build the protection.

13.6. Using the Text Interface – Syn Flood

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action)*.

Program location*:/aker/bin/firewall/fwflood*

Syntax:

```
Firewall Aker –
fwflood – Protection against SYN Flood configuration parameters
Usage: fwflood [activate | deactivate | show | help]
       fwflood [add | remove] <name>
       fwflood time <value>
```

Program help:

```
Firewall Aker –
fwflood – Protection against SYN Flood configuration parameters
Usage: fwflood [activate | deactivate | show | help]
       fwflood [add | remove] <name>
       fwflood time <value>


    active         = activates protection against SYN Flood
    deactivate     = deactivates protection against SYN Flood
    show     = shows the current configuration
```

Add = adds a new entity
remove = removes one entity

Time = Configure the maximum delay time to close a connection
help = Shows this message

To Include /remote

Name = Entity name to be protected or removed

For time:
Value = Maximum delay time in a unit of 500ms

Example 1: (Viewing the configuration)

```
#/aker/bin/firewall/fwflood shows configuration parameters
-------------------------------------
SYN Flood protection against: activated
Delay time   : 6 (x 500 ms)
List of entity selected to be protected:
-------------------------------------
NT1                                    (Host)
NT3                                    (Host)
```

13.7. Using the Remote Interface for Anti-Spoofing

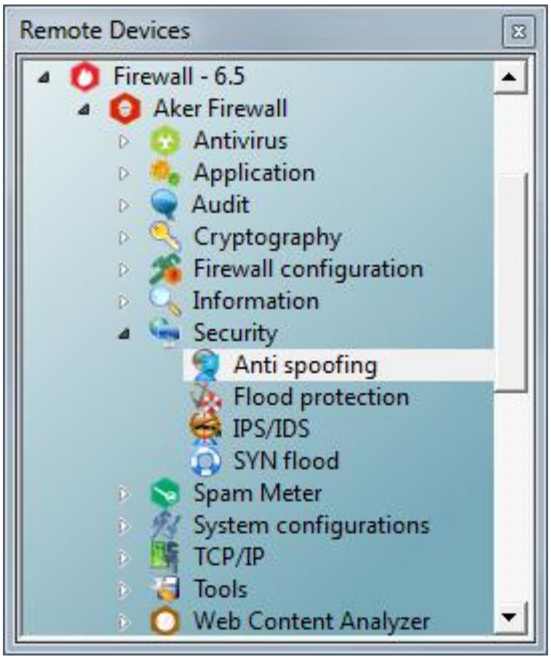
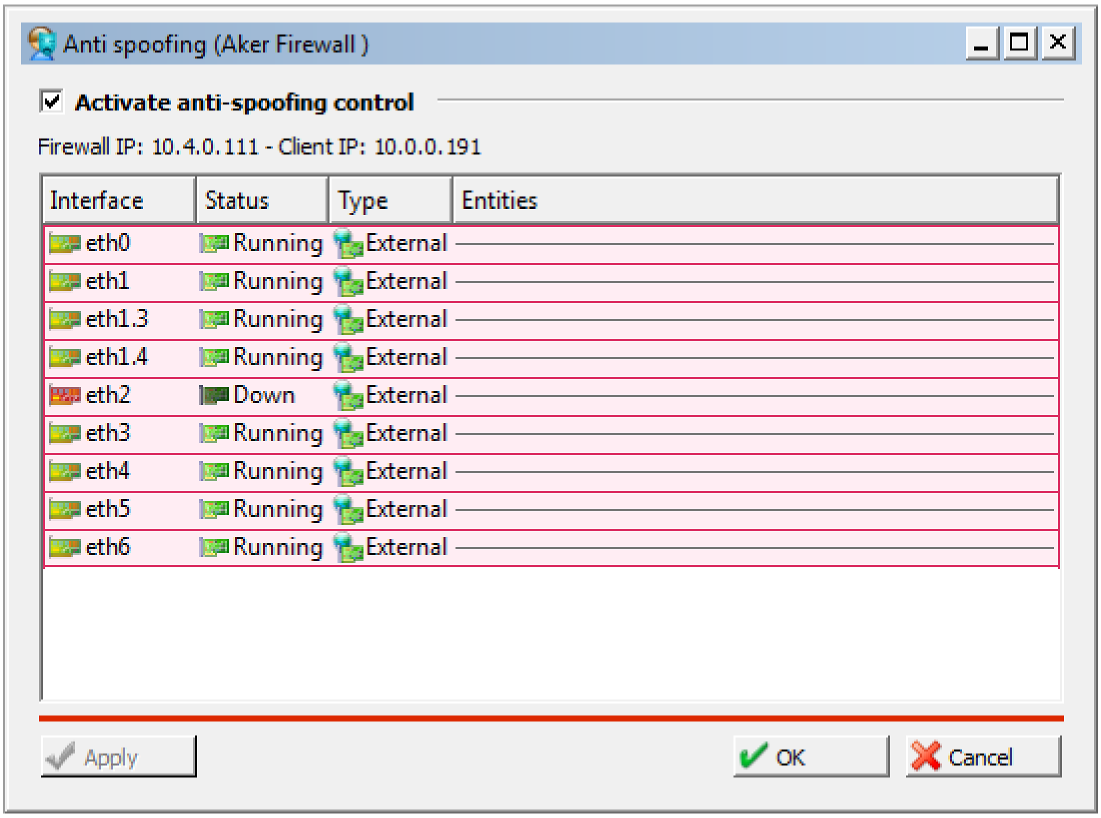

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Anti spoofing
Flood protection
IPS/IDS
SYN flood
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 307 – Access window: Anti-Spoofing.

- Click on the *Security menu* in the firewall window.
- Choose *Anti Spoofing*.

Anti-Spoofing configuration window



Anti spoofing (Aker Firewall)

☑ **Activate anti-spoofing control**

Firewall IP: 10.4.0.111 - Client IP: 10.0.0.191

Interface	Status	Type	Entities
eth0	Running	External	
eth1	Running	External	
eth1.3	Running	External	
eth1.4	Running	External	
eth2	Down	External	
eth3	Running	External	
eth4	Running	External	
eth5	Running	External	
eth6	Running	External	

Image 308 – Anti-Spoofing – Control activation

- The **OK** button will update the configuration parameters and close the window.
- The **Cancel** button will discard all changes and close the window.
- The **Apply** button will save all changes to the firewall and keep the window open.

Field meaning:

Activate anti-spoofing control: When this option is checked, it activates the Anti-Spoofing protection.
Interface: Corresponds to the interface entity registered in the firewall by the administrator.

Status: Shows the interface status whether it is up or down. This field cannot be edited.

Type: By default, this field is set as *External*. It can be changed to *Protected* by right-clicking on it. By doing this, it becomes possible to edit the *Entities* field next to it.

Protected means that the interface is connected to an Intranet and only packets whose source IP addresses are present in any of the entities specified in the rule will be accepted. *External* means that the interface is connected to the Internet and thus incoming packets with any source addresses will be accepted, except those that belong to any entity listed in any rule of an interface marked as *Protected*.

Entities: When an entity is defined as *Protected*, it is necessary to include in this field a list of all networks and/or hosts that are connected to this interface.

13.8. Using the text interface – Flood Protection

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action).*

Program location:/aker/bin/firewall/fwmaxconn

Syntax:

```
Aker Firewall
Usage: fwmaxconn help
    fwmaxconn show
    fwmaxconn add <pos> <source> <destination> <service> <n_conns>
    fwmaxconn remove <pos>
    fwmaxconn < enable | disable > <pos>

the parameters are:
        pos: position
        source: host/network where the connections are originated
        destination: host/network that connections are directed to
        service: network service for which there is a connection
        n_conns: maximum number of simultaneous connection from the same source
```

Example 1: (viewing configuration)

```
#/aker/bin/firewall/fwmaxconn show rule 01
--------
Source: Network_Internet
Destination: NT1
Services: HTTP
Connections: 5000

Rule 02
--------
Source: Network_Internet
Destination: NT3
Service: FTP
Connections: 10000
```

```
Rule 03
--------
Source: Network_Internet
Destination: Internal_Network
Services: Gopher
Connections: 100
```

13.9. Using the text interface – Anti Spoofing

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action).*

Program location*:/aker/bin/firewall/fwifnet*

Aker Firewall

```
Use: fwifnet [help | show]
    fwifnet add interface <name_if> [external]
    fwifnet add network <name_if> <network> [network1] [network2] ...
    fwifnet remove [-f] interface <name_if>
    fwifnet remove network <name_if> <address_IP> <mask>
    fwifnet <enable | disable>
```

Program help:

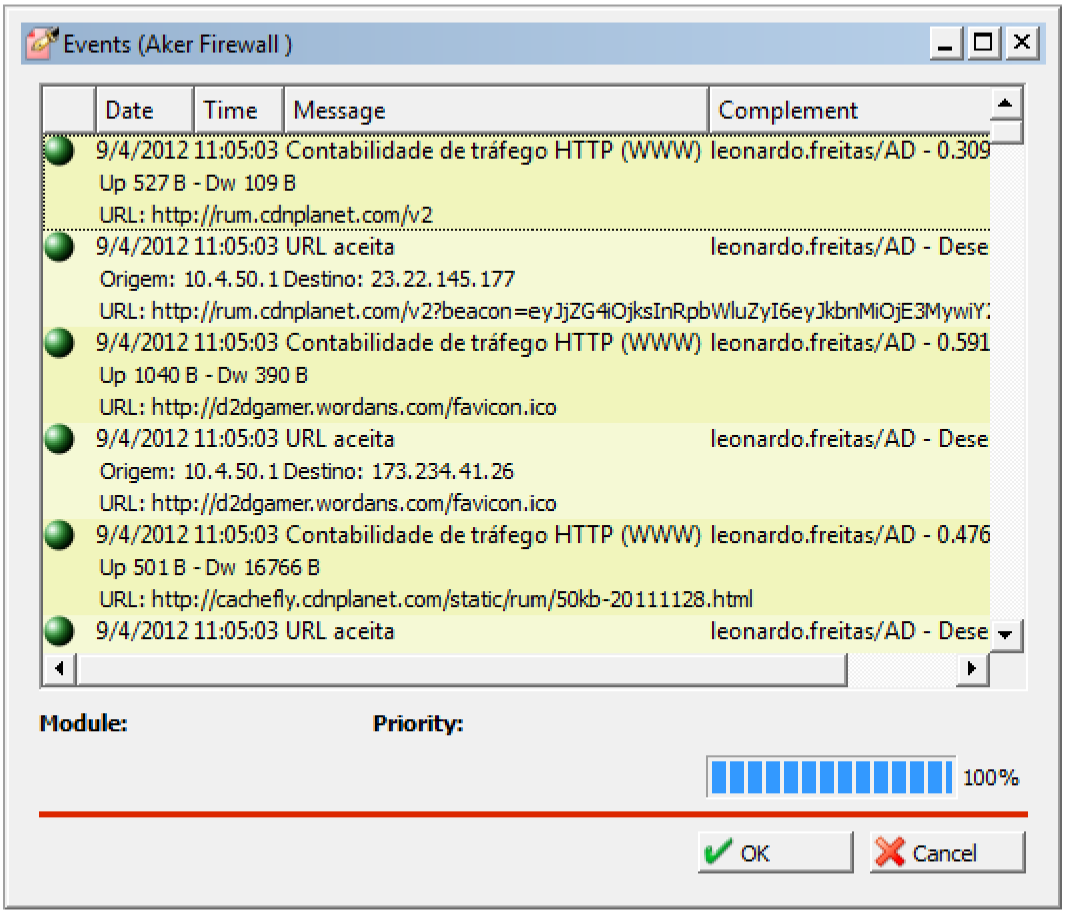
```
Use: fwifnet [help | show]
    fwifnet add interface <name_if> [external]
    fwifnet add network <name_if> <network> [network1] [network2] ...
    fwifnet remove [-f] interface <name_if>
    fwifnet remove network <name_if> <address_IP> <mask>

to add/remove:
    interface: network interface name selected to be controlled
    external: if this word is present, the interface will be considered external by the
firewall

    network: a network allowed in an interface which is not external
```

Example 1*: (viewing configuration)*

```
#/aker/bin/firewall/fwifnet show

Firewall Aker – Version 6.5
Anti-spoofing module status: enabled
Registered Interface: Interf_DMZ
Allowed network: Network_DMZInterface
```

registered: Interf_external (external)
Registered Interface: Interf_internal
Allowed network: Internal_Network

13.10. Block by excessive invalid logins attempts



```
    Date      Time     Message                           Complement
●  9/4/2012 11:05:03 Contabilidade de tráfego HTTP (WWW) leonardo.freitas/AD - 0.309
    Up 527 B - Dw 109 B
    URL: http://rum.cdnplanet.com/v2
●  9/4/2012 11:05:03 URL aceita                          leonardo.freitas/AD - Dese
    Origem: 10.4.50.1 Destino: 23.22.145.177
    URL: http://rum.cdnplanet.com/v2?beacon=eyJjZG4iOjksInRpbWluZyI6eyJkbnMiOjE3MywiY
●  9/4/2012 11:05:03 Contabilidade de tráfego HTTP (WWW) leonardo.freitas/AD - 0.591
    Up 1040 B - Dw 390 B
    URL: http://d2dgamer.wordans.com/favicon.ico
●  9/4/2012 11:05:03 URL aceita                          leonardo.freitas/AD - Dese
    Origem: 10.4.50.1 Destino: 173.234.41.26
    URL: http://d2dgamer.wordans.com/favicon.ico
●  9/4/2012 11:05:03 Contabilidade de tráfego HTTP (WWW) leonardo.freitas/AD - 0.476
    Up 501 B - Dw 16766 B
    URL: http://cachefly.cdnplanet.com/static/rum/50kb-20111128.html
●  9/4/2012 11:05:03 URL aceita                          leonardo.freitas/AD - Dese
```

Module: **Priority:**

Image 309 – Block by excessive invalid logins attempts – Events.

The firewall standard configuration comes with blocking by excessive invalid login attempts via control center. In case an IP attempt to connect three times with invalid users or passwords, the firewall will not allow connections for a period of time.

In the *Audit menu*, in *log window*, log events are created and can be seen, they have information such as the block time and the IP that attempt to connect.

Configuring the system actions

14. Configuring the system actions

This chapter shows hot to configure the system automatic responses for previously determined situations.

What are system actions?

Aker Firewall has a mechanism that allows the creation of automatic responses for specific situations. These automatic responses are configured by the administrator in a series of possible independent actions that will be performed when a pre-determined situation occur.

What are the system actions for?

The actions purpose is to make a high interaction degree between the firewall and the administrator as possible. Its usage allows, for an example, the execution of a program capable of paging the administrator when the firewall detects an attack. Therefore, the administrator will be capable of taking an immediate action, even if he is not monitoring the firewall at the moment.

14.1. Using the remote interface

To gain access to the *Action* window follow the steps below:

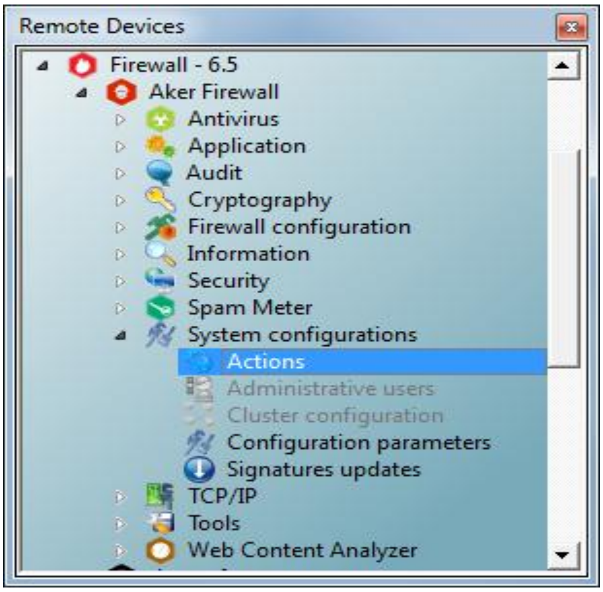

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
Actions
Administrative users
Cluster configuration
Configuration parameters
Signatures updates
TCP/IP
Tools
Web Content Analyzer

Image 310 – Access window – Actions.

- Click on the *System configurations* menu*;*
- Select *Actions*.

The actions configuration window

When this option is selected, the window that allows the configuration of actions to be taken by the system will be displayed. For each log and event message and for the packets which do not match any rule it is possible to set independent actions.

The window displayed will have this format:

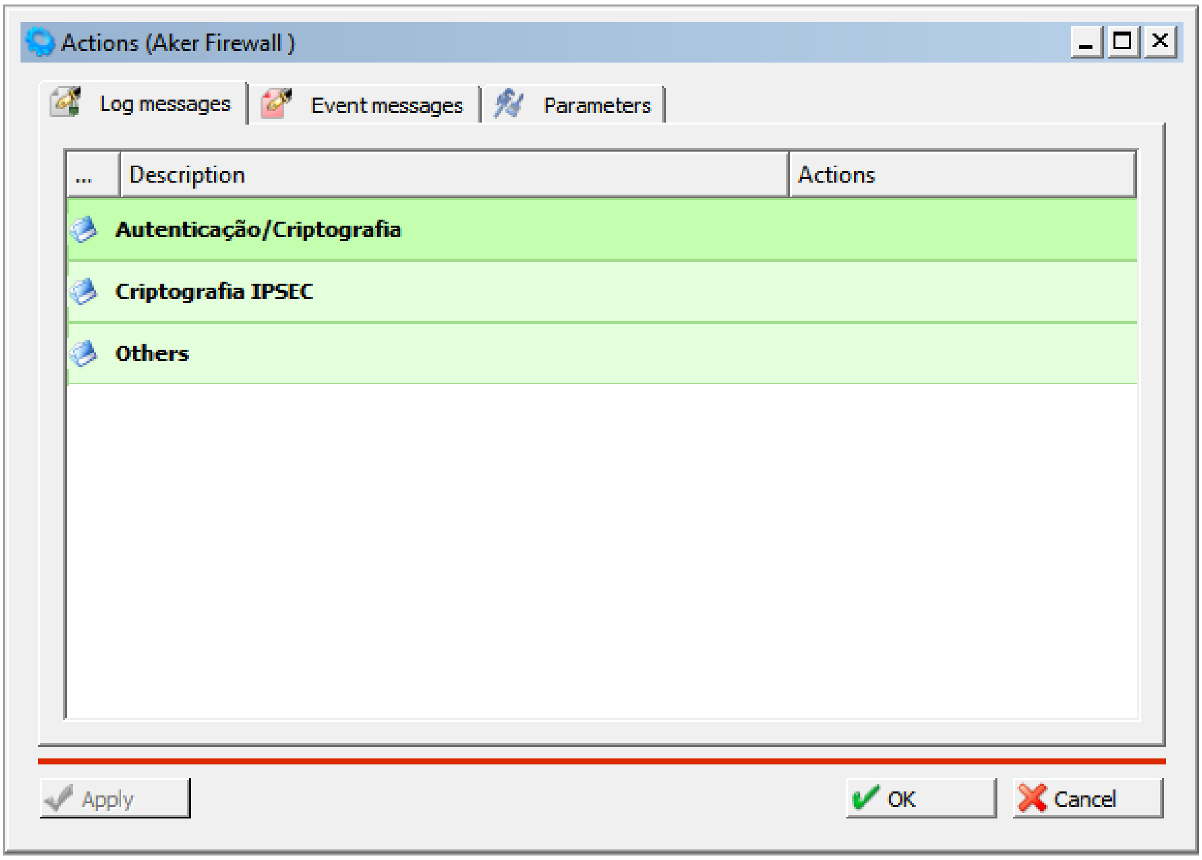

Actions (Aker Firewall)
Log messages
Event messages
Parameters
...
Description
Actions
Autenticação/Criptografia
Criptografia IPSEC
Others
Apply
OK
Cancel

Image 311 – Actions (Log messages)

To select the actions to be performed for the messages displayed in the window, right-click on the messages. For each selected action, a corresponding icon will be displayed.

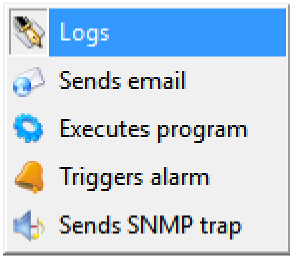

Logs
Sends email
Executes program
Triggers alarm
Sends SNMP trap

Image 312 – Access window (Actions- Options menu)

For each message that has the icon of an action, the correspondent action will be taken by the firewall when the message occurs. The following actions are allowed:

- **Logs**: If this option is active, every time the corresponding message occurs, it will be logged by the firewall.
- **Sends Mail**: If this option is active, an e-mail will be sent when the corresponding message occurs (the e-mail address configuration will be displayed in the next section).
- **Executes Program**: If this option is active, a program defined by the administrator will be executed every time the corresponding message occurs (the configuration of the path of the program to be executed will be displayed in the next section).
- **Triggers alarm**: If this option is active, the firewall will show an alert window every time the corresponding message occurs. This alert window will be displayed on the host where the Remote Interface is running and, if the host allows, a warning sound will also be produced. If the Remote Interface is not active, no messages will be displayed and this option will be ignored (this action is particularly useful to call the administrator's attention when an important message occurs).
- **Sends SNMP trap**: If this option is active, an SNMP Trap will be sent to the SNMP manager every time the corresponding message occurs (the configuration of the parameters to send traps will be displayed in the next section).

It is not possible to change the actions for the firewall initialization event message (message number 43). This message will always have only the Log option as configured actions.

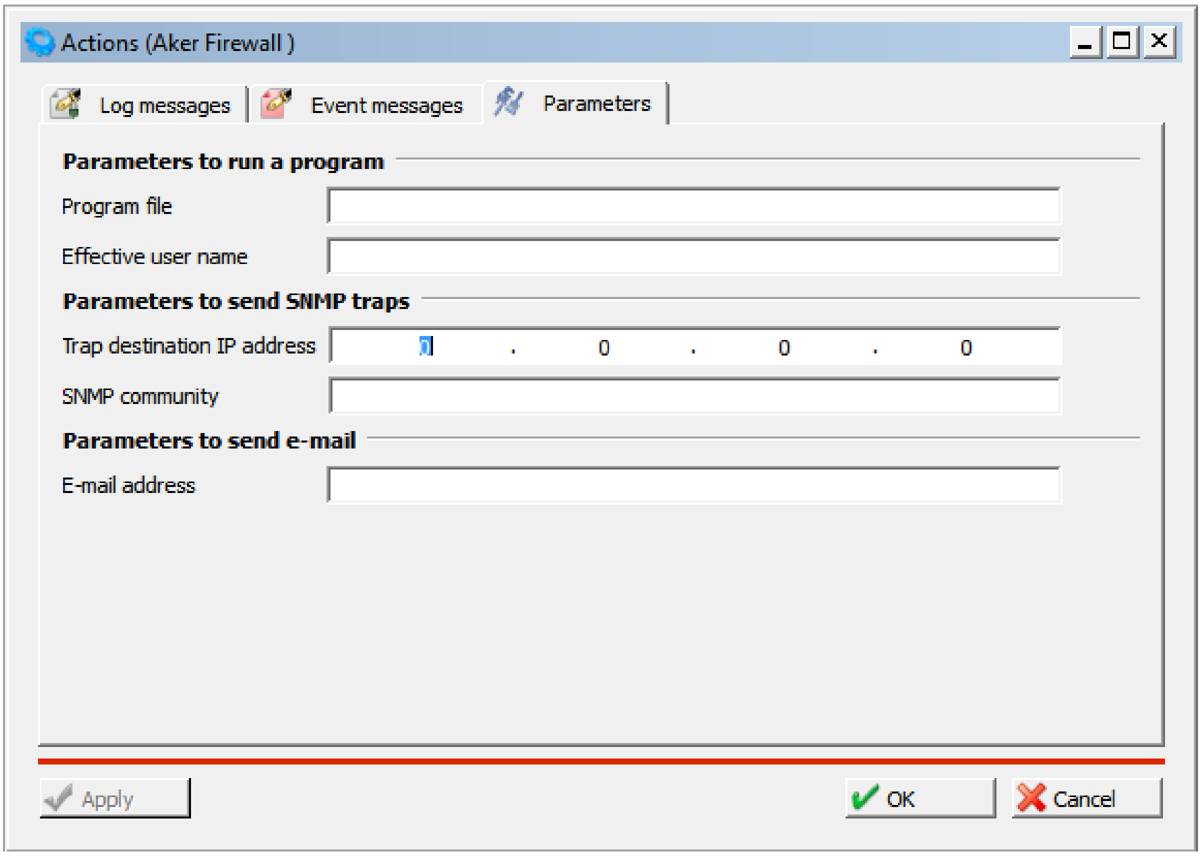
Meaning of the actions window buttons

- The **OK** button will close the actions window and apply the changes done.
- The **Cancel** button will close the window and discard the changes done.
- The **Apply** button will apply the changes but keep the window open.

The parameters configuration window

In order to get the system to take the actions, it is necessary to configure certain parameters (for example, for the firewall to send an e-mail, it is necessary to configure the address). These parameters are configured through the parameters configuration in the actions window.

This window is displayed when the **Parameters** tab in the messages window is clicked. It has the following format:



Parameters to run a program

Program file

Effective user name

Parameters to send SNMP traps

Trap destination IP address: 0 . 0 . 0 . 0

SNMP community

Parameters to send e-mail

E-mail address

Image 313 – Actions (Parameters)

Meaning of the parameters:

- **Parameters to run a program**

  Program file: This parameter configures the name of the program that will be run by the system, when an action with the option *Program* occurs. The full path name of the program must be typed. It is necessary to attempt to the fact that the program and all the directories on the path must have execution permission for the user who will execute it (which is configured in the next option).

  The program will receive the following parameters by the command line (in the same order as displayed):

  1. Name of the program being run (this is a standard for the unix operating system).
  2. Type of message (**1** – for log or **2 –** for event).
  3. Priority (**7** – debug, **6** – information, **5** – notice, **4** – warning or **3** – error).
  4. Number of the message that caused the execution of the program or **0** to indicate the cause was not a message. (in this case, the execution of the program was initiated by a rule)
  5. ASCII string with the complete text of the message (this string may have the line feed characters in it).

In the UNIX operating system, the slash "/" is used to specify the path of a program. It may confuse those who are used to the DOS/Windows environment, where the backslash is "\" is used.

Effective user name: This parameter indicates the identity of which the external program will be executed. The program will have the same privileges of this user.

This user must be a valid user, registered in Linux. It is necessary not to confuse him with the Aker Firewall users, which are useful only for the Firewall administration.

- **Parameters to send SNMP traps**

Trap destination IP address: This parameter configures the IP address of the SNMP manager to which the firewall must send the traps.

SNMP community: This parameter configures the name of the SNMP community that will be sent in the traps.

The sent SNMP traps will have the generic type **6** (*enterprise specific*) and the specific type **1** for log or **2** for events. They will be sent with the enterprise number **2549**, which is the number assigned by the IANA to the Aker.

There is a file called **/etc/firewall/mibs/AKER-MIB.TXT,** which brings information about Aker sub-tree in the global tree. This file is written on the ASN.1 notation.

- **Parameters to send e-mail**

E-mail address: This parameter configures the e-mail address of the user the email will be sent to. This user can be a user from the firewall itself or not (in this situation, it is necessary to write the complete address, for example user@aker.com.br).

If it is desired to send e-mails to several users, a list can be created and the name of the list can be inserted in this field.

It is important to notice that, if any of these fields are blank, the corresponding action will not be taken, even if it is active.

14.2. Using the text interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action*).

Program location: /aker/bin/firewall/fwaction

Sintax:

```
fwaction help
fwaction show
fwaction assign <number> [log] [mail] [trap] [program] [alert]
fwaction <program | user | community> [name]
fwaction ip [IP address]
fwaction e-mail [address]
```

Program help:

```
fwaction – Command line interface for configuring system actions
Usage: fwaction help
    fwaction show
    fwaction assign <number> [log] [mail] [trap] [program] [alert]
    fwaction <program | user  | community> [name]
    fwaction ip [IP address]
    fwaction e-mail [address]

    help      = shows this message
    show      = lists the messages and the actions assigned to each of them
    assign    = assigns actions for a specific message
    program   = defines the name of the program to be run
    user      = defines the name of the user that will run the program
    community = defines the name of the SNMP community for trap
generation
    ip       = defines the IP address of the SNMP server that will receive
               the traps
    e-mail    = defines the name of the user that will receive the e-mails

For the assign command:
    number    = number of the message which the action will be assigned to
               (the number of each message is displayed on the left when
                the option show is selected)
    log      = Logs each message generated
    mail      = Sends an e-mail for each message generated
    trap      = Sends a SNMP trap for each message generated
    program   = Executes program for each message generated
```

alert = Open an alert window for each message generated

Example 1: (configuring the parameters for e-mails sending and program execution)

```
#fwaction e-mail root
#fwaction program /etc/pager
#fwaction user nobody
```

Example 2: (showing the complete configuration of the actions of the system)

```
#fwaction show
General Conditions:

00 – Packet did not match any rule
>>>> Log

Log messages:


01 – Possible fragmentation attack
  >>>> Log
  02 – Source routed IP packet
  >>>> Log
  03 – Land attack
  >>>> Log
  04 – Connection is not present in the dynamic table
  >>>> Log
  05 – Packet was received from an invalid interface
  >>>> Log
  06 – Packet was received from an unknown interface
  >>>> Log
  07 – Control connection is not open
  >>>> Log


(...)

237 –  Secure Roaming has found an error

>>>> Log
238 – Secure Roaming has found a fatal error
>>>> Log
239 – Users who are responsible for the Configuration Manager
>>>> Log

Configuration parameters:

program: /aker/bin/pager
```

```
user: nobody
e-mail: root
community:
ip:
```

Due to a large number of messages, only the first and the last ones are displayed. The real program will show all of them when executed.

Example 3: (assigning actions to the *Packet did not match any rule* message and showing the messages)

```
#fwaction assign 0 log mail alert
#fwaction show
General Conditions:

00 – Packet did not match any rule
>>>> Log Mail Alert

Log messages:

01 – Possible fragmentation attack
>>>> Log
02 – Source routed IP packet
>>>> Log
03 – Land attack
>>>> Log
04 – Connection is not present in the dynamic table
>>>> Log
05 – Packet was received from an invalid interface
>>>> Log
06 – Packet was received from an unknown interface
>>>> Log
07 – Control connection is not open
>>>> Log
```

```
(...)

237 –  Secure Roaming has found an error

>>>> Log
238 – Secure Roaming has found a fatal error
>>>> Log
239 – Users who are responsible for the Configuration Manager
>>>> Log
```

```
Configuration parameters:

program : /aker/bin/pager
user : nobody
e-mail : root
community:
ip :
```

Due to a large number of messages, only the first and the last ones are displayed. The real program will show all of them when executed.

Example 4: (canceling all the actions for the *Source routed IP packet* message and showing the messages)

```
#fwaction assign 2
#fwaction show
General Conditions:

00 – Packet did not match any rule
>>>> Log Mail Alert

Log messages:

01 – Possible fragmentation attack
>>>> Log Mail
02 – Source routed IP packet
>>>>
03 – Land attack
>>>> Log
04 – Connection is not present in the dynamic table
>>>> Log
05 – Packet was received from an invalid interface
>>>> Log
06 – Packet was received from an unknown interface
>>>> Log
07 – Control connection is not open
>>>> Log
```

```
(...)

237 –  Secure Roaming has found an error

>>>> Log
238 – Secure Roaming has found a fatal error
>>>> Log
```

```
239 – Users who are responsible for the Configuration Manager
>>>> Log


Configuration parameters:

program: /aker/bin/pager
user: nobody
e-mail: root
community:
ip:
```

Due to a large number of messages, only the first and the last ones are displayed. The real program will show all of them when executed.

Viewing the system log

15. Viewing the system log

In this chapter, we will show hot to view the system log, an essential resource for attack detection, firewall tracking and monitoring, and during system configuration phone.

What is the system log?

The log is where the firewall stores all information about packets received. It may contain records generated by any of the three main modules: packet filter, network address translation, and encryption/authentication. The type of information stored in the log depends on the firewall configuration, but basically, it includes information about accepted, rejected and discarded packets, packet errors, and network address translation information.

Among all the data stored in the log, information about discarded and rejected packets is, possibly, the most important. Because it is through the analysis of these data that we may determine eventual attempts of invasion, unauthorized service use, and configuration errors, among others.

What is a log filter?

Even though the system is configured to record all kinds of information, sometimes a specific type of information is of more interest (for example, the rejected attempts to use the POP3 service of a specific host, on a given day, or still, the attempts that were indeed accepted). The log filter is a mechanism offered by Aker Firewall, to create different views of the whole set of log records, making it easier to obtain the desired information.

The filter only shows information previously registered in the log. If specific information is targeted, the log system must be configured to register it first, and then, a filter is used to view it.

15.1. Using the Remote Interface

To access the log windows follow the step below:

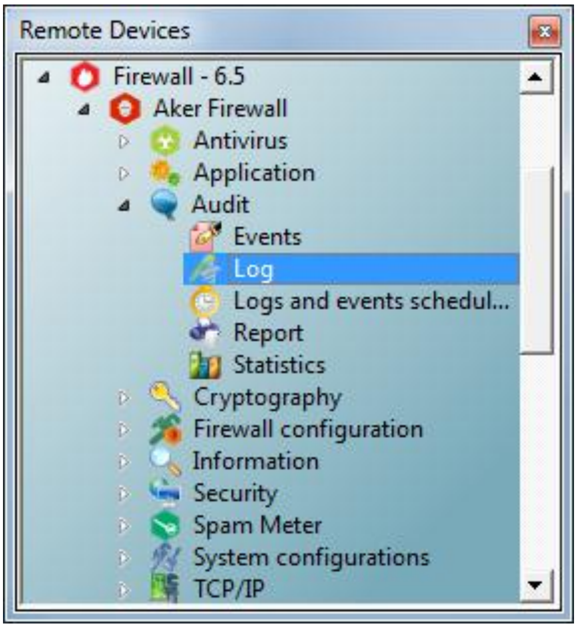

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Events
Log
Logs and events schedul...
Report
Statistics
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 314 – access window (log)

- Click on the *Audit* menu on the firewall you desire to see;
- Select *Log*.

The Log toolbar

Every time the Log option is selected, the Log bar comes up automatically. It is located next to other bars .The log bar may be dragged and left floating anywhere over the Log information.

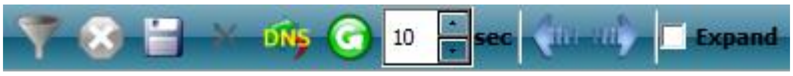

DNS
10
sec
Expand

Image 315 – Log toolbar.

Meaning of icons:

Opens the firewall Log Filter window.

Image 316 – *Firewall Log Filter* icon.

This icon will only show up when the firewall is performing a search in the Log. It allows interruption of the search.

Image 317 – *Interrupt firewall search* icon.

Exports the Log to several file formats.

Image 318 – *Export log* icon.

Erases the firewall Log.

Image 319 – *Erase firewall log* icon.

Performs a reverse resolution of the IP displayed by the Log.;

Image 320 – *Reverse resolution of IP* icon

The log screen is refreshed at every specified period of time, defined in the field next to it (described below);

Image 321 – *Log screen refresh* icon.

Defines the time that log information window will be updated by the firewall.

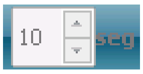


Image 322 – *Log update time* icon.

Goes through the Log;

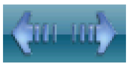


Image 323 – *Go through log* icon.

Expands Log messages to show all the information.

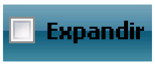
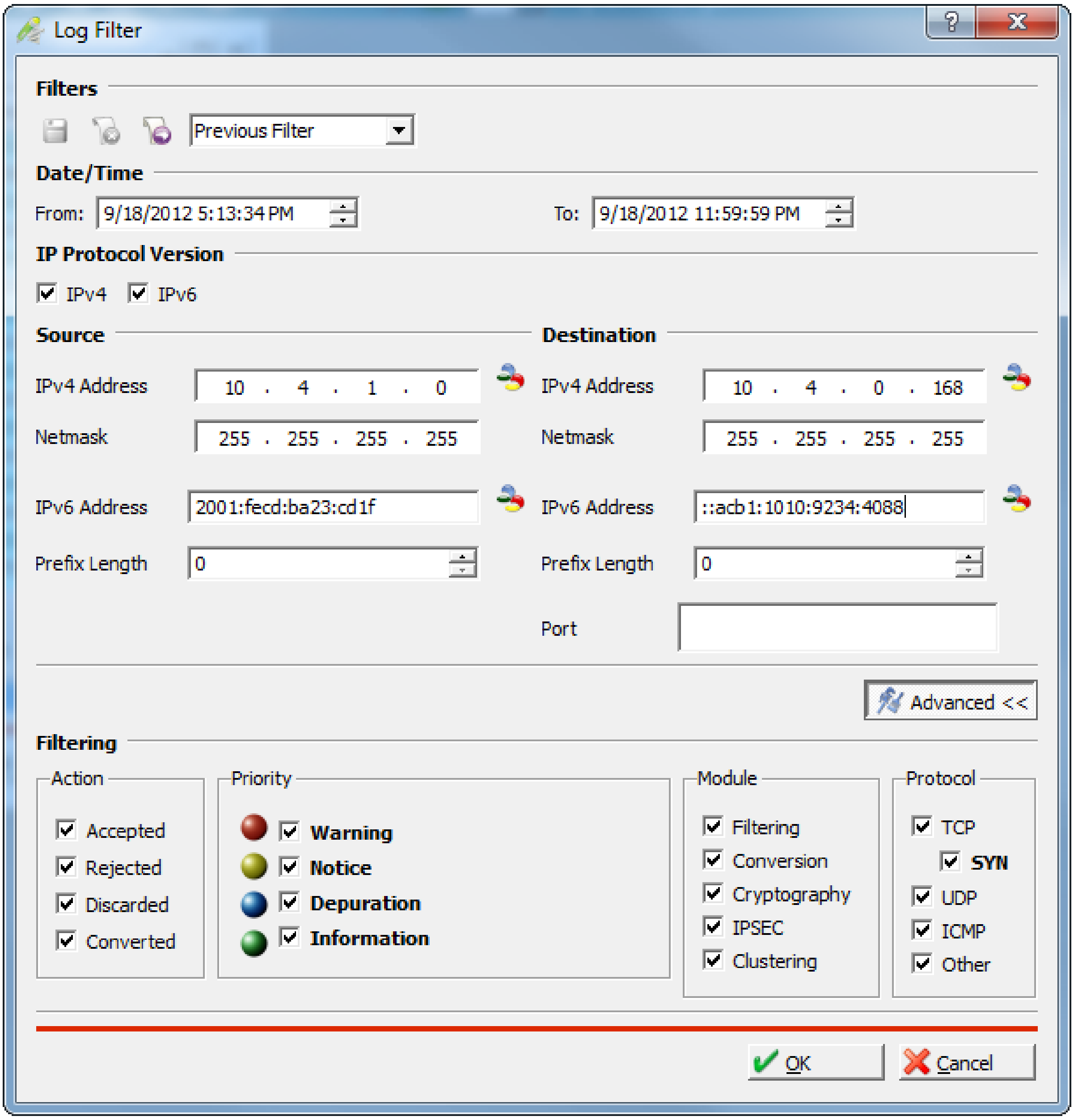


Image 324 – *Expand log messages* icon.

Log filter window



Filters

Previous Filter

Date/Time

From: 9/18/2012 5:13:34 PM
To: 9/18/2012 11:59:59 PM

IP Protocol Version

☑ IPv4 ☑ IPv6

Source

IPv4 Address 10 . 4 . 1 . 0
Netmask 255 . 255 . 255 . 255
IPv6 Address 2001:fecd:ba23:cd1f
Prefix Length 0

Destination

IPv4 Address 10 . 4 . 0 . 168
Netmask 255 . 255 . 255 . 255
IPv6 Address ::acb1:1010:9234:4088
Prefix Length 0
Port

Filtering

Action
☑ Accepted
☑ Rejected
☑ Discarded
☑ Converted

Priority
☑ **Warning**
☑ **Notice**
☑ **Depuration**
☑ **Information**

Module
☑ Filtering
☑ Conversion
☑ Cryptography
☑ IPSEC
☑ Clustering

Protocol
☑ TCP
☑ **SYN**
☑ UDP
☑ ICMP
☑ Other

Image 325 – Log filter window.

The **Save**, **Remove**, and **New** buttons are located at the top part of the window. It allows saving a search profile which might be used later by the administrator.

To save a log filter, do the following:

1. Fill in all the fields in the desired way.
2. Define a name for the field **Filters**
3. Click on the Save button.

To apply a saved filter, select its name in the **Filters** field. All fields will be automatically filled with the saved data.

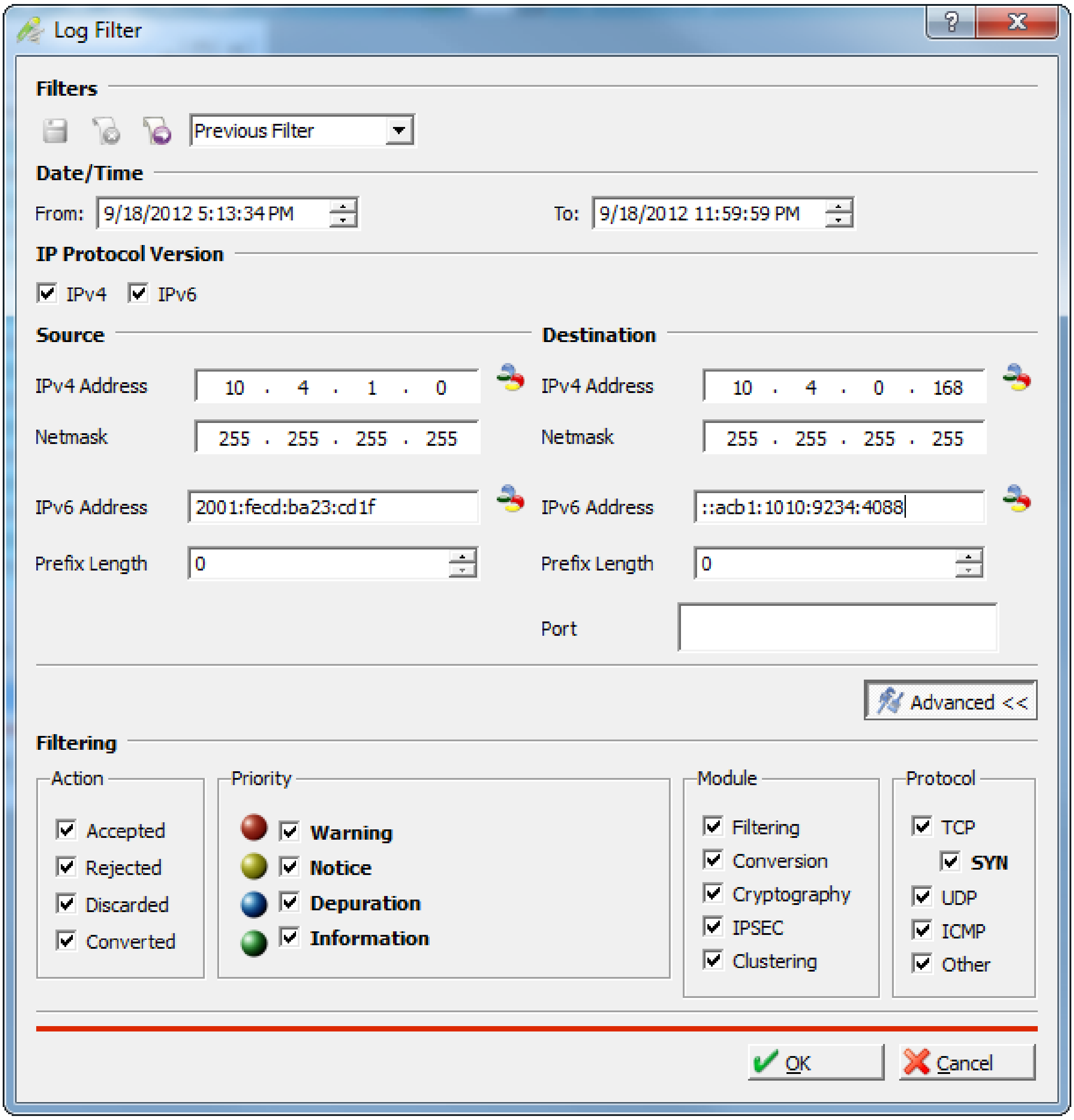
To remove a filter, follow the steps below:

1. Select the filter to be removed in the **Filters** field.
2. Click on **Remove**.

The default filter is configured to show all records of the current day. To view information of other time periods, configure **From** and **To** fields, in the Date/Time area, to the desired dates (the initial and the final dates will be included in the view).

If you want to target source and/or destination addresses belonging to a specific set of hosts, you can use the IP / Mask fields, or the Entity button to specify it

The icon allows the type of filtering that will be performed, the following fields will be displayed on the window: packet origin IP and Mask, and packet destination IP and Mask. These fields may be used to specify the source set and/or the destination set. In this case, it is possible to select an entity, in each one of these fields that will be used to specify origin and destination sets. Buttons can be selected independently. This way, the filtering criteria can be based on one or both, an entity in the origin set or on the IP and Mask of the destination set.



Log Filter

Filters

Previous Filter

Date/Time

From: 9/18/2012 5:13:34 PM

To: 9/18/2012 11:59:59 PM

IP Protocol Version

☑ IPv4 ☑ IPv6

Source

IPv4 Address: 10 . 4 . 1 . 0

Netmask: 255 . 255 . 255 . 255

IPv6 Address: 2001:fecd:ba23:cd1f

Prefix Length: 0

Destination

IPv4 Address: 10 . 4 . 0 . 168

Netmask: 255 . 255 . 255 . 255

IPv6 Address: ::acb1:1010:9234:4088

Prefix Length: 0

Port:

Advanced <<

Filtering

Action: ☑ Accepted ☑ Rejected ☑ Discarded ☑ Converted

Priority: ☑ **Warning** ☑ **Notice** ☑ **Depuration** ☑ **Information**

Module: ☑ Filtering ☑ Conversion ☑ Cryptography ☑ IPSEC ☑ Clustering

Protocol: ☑ TCP ☑ **SYN** ☑ UDP ☑ ICMP ☑ Other

OK Cancel

Image 326 – Log filter window.

To monitor a specific service, just write its number in the **Port** field. From then on, only entries with the specified service will be displayed. It is also important to select the protocol associated with the service, in the protocol field. To access it, press the *advanced* button.

To specify a service in the TCP and UDP protocols, it is necessary to put the destination port number, associated to the service, in this field. In ICMP, it is necessary to put the type of the service. For other protocols, the number of the desired protocol is needed.

Besides these fields, there are other options that may be combined to further restrict the type of information displayed:

Action:

It represents the action taken by the system to deal with a specific packet. The following options can be independently selected:

- **Accepted**

  Shows packets accepted by the firewall.

- **Rejected**

  Shows the packets rejected by the firewall.

- **Discarded**

  Shows packets discarded by the firewall.

- **Converted**

  Shows the messages related to network address translation.

Priority:

Different types of messages have different priorities. As higher the priority assigned to a specific log, greater shall be its importance. A list of all possible priorities is displayed below, ordered from the most important to the least important (if the firewall is configured to send a copy of the log to the Syslogd (logging subsystem), the Syslog message generation will also follow this priority scheme):

- **Warning**

  Logs with this priority level usually indicate an attack or a very serious situation (such as encryption channel configuration error). This type of record is always preceded by a message with more information about it.

- **Notice**

  Packets that were rejected or discarded by the system are usually classified with this priority level. They either matched a rule configured to reject or discard them, or they did not fit any rule. In some situations, they may be preceded by explanatory messages.

- **Information**

  These logs add useful, non-critical information to the Firewall administration. No explanatory message precedes them. This priority level is usually associated to packets accepted by the firewall.

- **Debug**

  Logs with this priority level are usually useful only when the system is being configured. Messages of network address translation are examples with this priority level.

Module:

This option is for independently viewing the logs generated by each of the three main system modules: (1) Packet Filter, (2) Network Address Translator and (3) Encryption, IPsec, and Clustering module.

Protocol:

This field specifies the protocol of the logs that will be displayed. The options are:

- **TCP**

  Displays logs generated through TCP packets. If this option is checked, the TCP/SYN option will be automatically unchecked.

- **TCP/SYN**

  Displays logs generated through the TCP connection initiation packets. If this option is checked, the TCP option will be automatically unchecked.

- **UDP**

  Displays logs generated through UDP packets

- **ICMP**

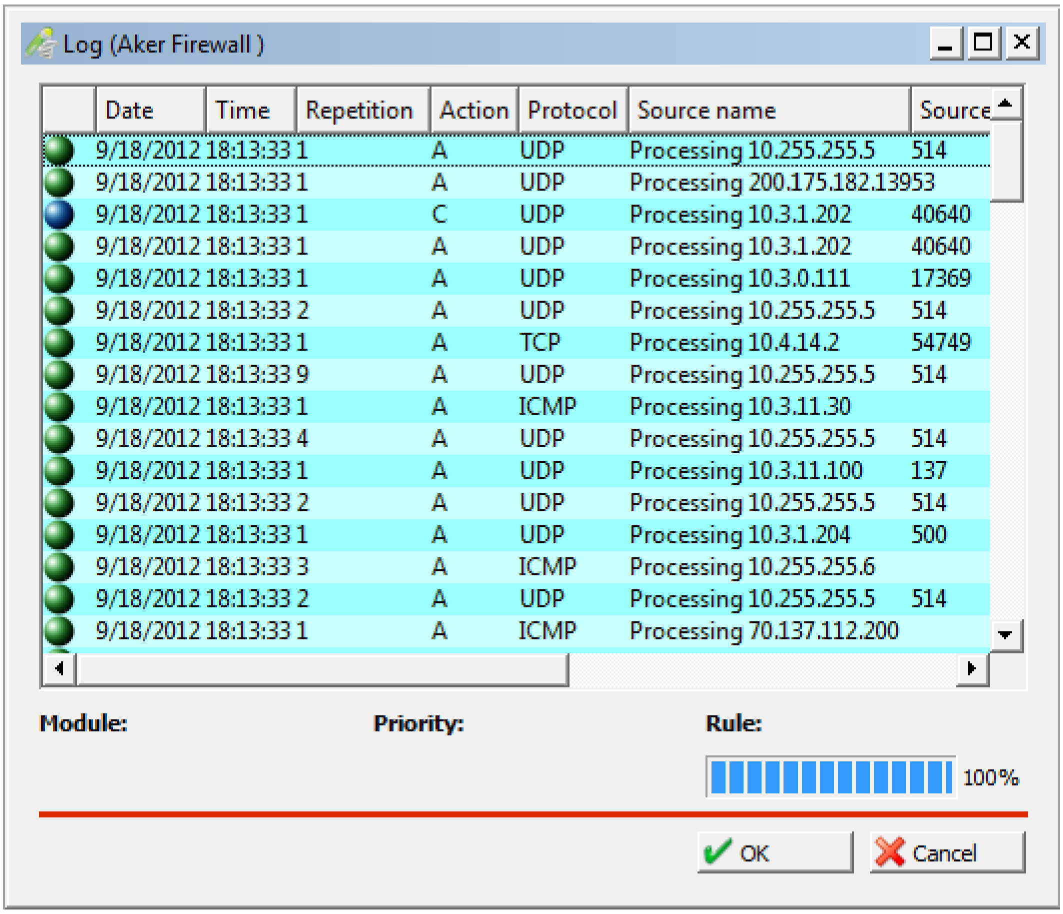
  Displays logs generated through ICMP packets.

- **Other**

  Packets generated by protocols other than TCP, UDP, and ICMP will be displayed. It is possible to further restrict the protocol to be displayed, by specifying its number, through the **Destination Port** or **Type of Service** fields.

- The **OK** button will apply the chosen filter, and show the filtered information on the Log window.
- The **Cancel** button will cancel the filtering operation, and the Log window will display the same information it has shown before.

Log window



	Date	Time	Repetition	Action	Protocol	Source name	Source
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 200.175.182.13953	
🔵	9/18/2012	18:13:33	1	C	UDP	Processing 10.3.1.202	40640
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 10.3.1.202	40640
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 10.3.0.111	17369
🟢	9/18/2012	18:13:33	2	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	TCP	Processing 10.4.14.2	54749
🟢	9/18/2012	18:13:33	9	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	ICMP	Processing 10.3.11.30	
🟢	9/18/2012	18:13:33	4	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 10.3.11.100	137
🟢	9/18/2012	18:13:33	2	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	UDP	Processing 10.3.1.204	500
🟢	9/18/2012	18:13:33	3	A	ICMP	Processing 10.255.255.6	
🟢	9/18/2012	18:13:33	2	A	UDP	Processing 10.255.255.5	514
🟢	9/18/2012	18:13:33	1	A	ICMP	Processing 70.137.112.200	

Image 327 – List several log entries.

The Log Window will be displayed after a new filter is applied. It has a list of several entries. All entries have the same format, however depending on the generating packet protocol some fields may be missing. Some entries will also be preceded by a special text message, with additional information about the record (the meaning of each type of record will be displayed in the next section).

Important notes:

- Records will be displayed 100 at a time.
- Only the first 10,000 logs matching the chosen filter will be displayed. The remainder can be accessed by exporting the log to a file, or by using a filter that generates fewer logs.
- On the left of each message, a colored icon will be displayed, representing its priority. A legend is presented below:

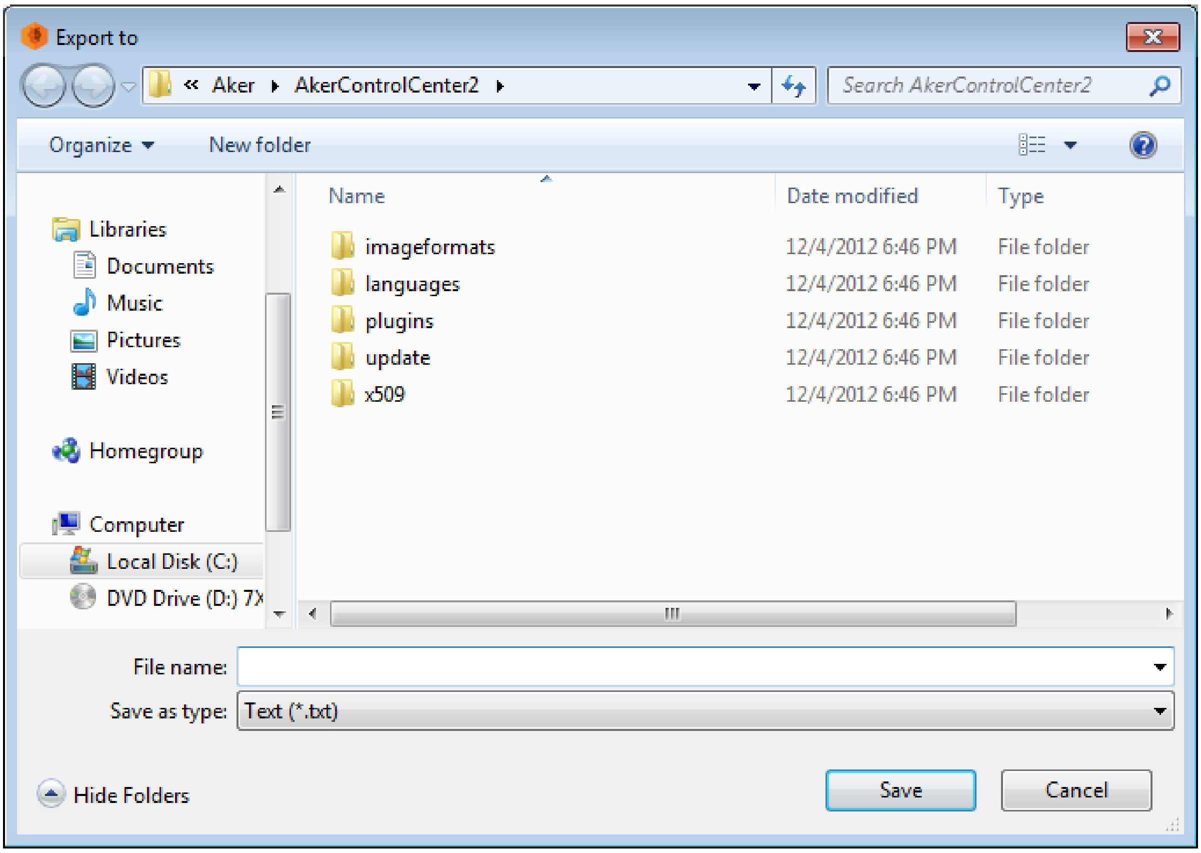
Blue	Debug
Verde	Information
Yellow	Notice
Red	Warning

- Left click on a message additional information about the log will be displayed at the bottom of the screen.

If a log file is deleted, the only way to recover the information is restoring a backup copy.

Logs will be exported together with their additional messages if the Expand option is checked, and the option to export text file type is chosen. Otherwise, the log will be exported without messages.

This option is very useful when you want to send a copy of the log to someone else, to keep a text copy of important information, or to import a log by one of the log analyzers cited above. The following window will show up when the Export button is pressed:

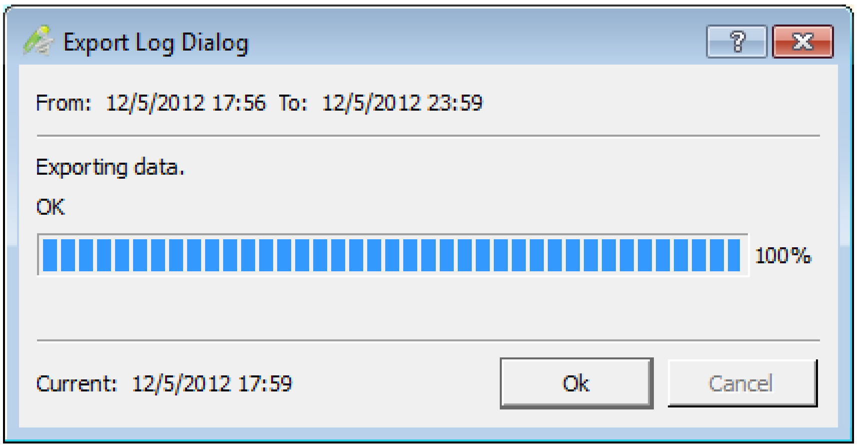

Export to
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize ▾
New folder
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
Hide Folders
Save
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder

File name:

Save as type: Text (*.txt)

Image 328 – Exporting the logs.



From: 12/5/2012 17:56 To: 12/5/2012 23:59

Exporting data.

OK

100%

Current: 12/5/2012 17:59

Image 329 – Export Log Dialog

To export the log content, name the file to be created, choose its type, and click on **Save**. To cancel the operation, click on **Cancel**

If a file with the same name already exists, it will be erased.

- The **Next** button, represented by a right pointing arrow in the toolbar, shows the next 100 records selected by the filter. If there are no more records, this option is disabled.
- The **Previous** button, represented by a left pointing arrow in the toolbar, shows the previous 100 records. If there are no previous records, this option is disabled.
- The **Help** button shows specific help for the Log Window.

15.2. Format and meaning of the fields of log records

Bellow follows the format description each record, followed by a description of each one of the fields. The record format is the same for the Remote Interface and for the Text Interface.

Records generated through the packet filter or through cryptography module.

Any of these records can be preceded by a special message. The full list of possible messages and its meaning is found in the **appendix A**.

- **TCP protocol**

  Record format:

  <Date> <Time> – <Repetition> <Action> TCP <Status> <Source IP > <Source Port> <Destination IP > <Destination Port> <Flags> <Interface>

Description of fields:

Date: Date that the record was generated.
Time: Time that the record was generated.
Repetition: Number of times that the record was repeated subsequently. This field is displayed in parentheses in the text interface.
Status: This field, which appears in parentheses in the text interface, consists of 1 to 3 letters. These letters have the following meanings:

A: Authenticated Packet
E: Encrypted Packet
S: Packet used for the key Exchange via SKIP or AKER-CDP

Action: This field indicates what action has been taken by the firewall related to the packet. The values are:

A: Indicates that the packet has been accepted by the firewall.
D: Indicates that the packet has been discarded.
R: Indicates that the packet has been rejected.

Source IP: Source IP address of the packet which has generated the record.
Source Port: Source Port of the packet which has generated the record.
Destination IP: Destination IP address of the packet which has generated the record.
Destination Port: Destination port of the packet which has generated the record.
Flags: TCP protocol flags present in the packet that has generated the record. This field consists of six independent letters. The presence of one letter indicates the corresponding flag to it, is already in the packet. The meanings of letters are:

S: SYN
F: FIN
A: ACK
P: PUSH
R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Firewall’s network interface where the packet was received.

- **UDP Protocol**

Record format:

<Date> <Time> – <Repetition> <Action> UDP <Status> <Source IP > <Source Port> <Destination IP> <Destination Port> <Interface>

Description of field:

Date: Date that the record was generated.
Time: Time that the record was generated.
Repetition: Number of times that the record was repeated subsequently. This field is displayed in parentheses in the text interface.
Status: This field, which appears in parentheses in the text interface, consists of 1 to 3 letters. These letters have the following meanings:

A: Authenticated Packet
E: Encrypted Packet
S: Packet used for the key Exchange via SKIP or AKER-CDP

Action: This field indicates what action has been taken by the firewall related to the packet. The values are:

A: Indicates that the packet has been accepted by the firewall.
D: Indicates that the packet has been discarded.
R: Indicates that the packet has been rejected.

Source IP: Source IP address of the packet which has generated the record.
Source Port: Source Port of the packet which has generated the record.
Destination IP: Destination IP address of the packet which has generated the record.
Destination Port: Destination port of the packet which has generated the record.
Flags: TCP protocol flags present in the packet that has generated the record. This field consists of six independent letters. The presence of one letter indicates the corresponding flag to it, is already in the packet. The meanings of letters are:

S: SYN
F: FIN
A: ACK
P: PUSH
R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Firewall's network interface where the packet was received.

ICMP Protocol

Record format:

<Date> <Time> – <Repetition> <Action> ICMP <Status> <Source IP > <Destination IP> <Type of service> <Interface>

Description of fields:

Date: Date that the record was generated.
Time: Time that the record was generated.
Repetition: Number of times that the record was repeated subsequently. This field is displayed in parentheses in the text interface.
Status: This field, which appears in parentheses in the text interface, consists of 1 to 3 letters. These letters have the following meanings:

A: Authenticated Packet
E: Encrypted Packet
S: Packet used for the key Exchange via SKIP or AKER-CDP

Action: This field indicates what action has been taken by the firewall related to the packet. The values are:

A: Indicates that the packet has been accepted by the firewall.
D: Indicates that the packet has been discarded.
R: Indicates that the packet has been rejected.

Source IP: Source IP address of the packet which has generated the record.
Source Port: Source Port of the packet which has generated the record.
Destination IP: Destination IP address of the packet which has generated the record.
Destination Port: Destination port of the packet which has generated the record.
Flags: TCP protocol flags present in the packet that has generated the record. This field consists of six independent letters. The presence of one letter indicates the corresponding flag to it, is already in the packet. The meanings of letters are:

S: SYN
F: FIN
A: ACK
P: PUSH
R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Firewall’s network interface where the packet was received.

- **Other protocols**

Record format:

<Date> <Time> – <Repetition> <Action> <Protocol> <Status> <Source IP> <Destination IP> <Interface>

Description of fields:

Date: Date that the record was generated.
Time: Time that the record was generated.
Repetition: Number of times that the record was repeated subsequently. This field is displayed in parentheses in the text interface.
Status: This field, which appears in parentheses in the text interface, consists of 1 to 3 letters. These letters have the following meanings:

A: Authenticated Packet
E: Encrypted Packet
S: Packet used for the key Exchange via SKIP or AKER-CDP

Action: This field indicates what action has been taken by the firewall related to the packet. The values are:

A: Indicates that the packet has been accepted by the firewall.
D: Indicates that the packet has been discarded.
R: Indicates that the packet has been rejected.

Source IP: Source IP address of the packet which has generated the record.
Source Port: Source Port of the packet which has generated the record.
Destination IP: Destination IP address of the packet which has generated the record.
Destination Port: Destination port of the packet which has generated the record.
Flags: TCP protocol flags present in the packet that has generated the record. This field consists of six independent letters. The presence of one letter indicates the corresponding flag to it, is already in the packet. The meanings of letters are:

S: SYN
F: FIN
A: ACK
P: PUSH
R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Firewall's network interface where the packet was received.

Records generated by the address translation

Record format:

<Date> <Time> – <Repetition> C <Protocol> <Source IP > <Source Port> <Translated IP> <Translated Port>

Description of records field

Date: Date that the record was generated.
Time: Time that the record was generated.
Repetition: Number of times that the record was repeated subsequently. This field is displayed in parentheses in the text interface.
Protocol: It Is the packet protocol that has generated the record, it might be TCP or UDP.
Source IP: Source IP address of the packet which has generated the record.
Source Port: Source Port of the packet which has generated the record.
Translated IP: IP address that the source address of packet was translated for.

Translated Port: Port that the source port of packet was translated for.

15.3. Using the text interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action*. All GUI functions are available, except for the message filtering option. Another limitation is that it is not possible, through the Text Interface, to access the additional information obtained when we select events message in the GUI, or when we activate the *Expand* option

Program location: /aker/bin/firewall/fwlog

Syntax:

Aker Firewall
fwlog delete [log | log6 | events] [<initial_date> <end_date>]

fwlog show [log | events] [local | cluster] [<initial_date> < end_date>] [priority]

Program help:

Usage: fwlog help
fwlog delete [log | log6 | events] [<initial_date> <end_date>]
fwlog show [log | log6 | events] [local | cluster] [<initial_date> <end_date>] [priority]

fwlog – Text Interface used to view log and events
show = lists records of the specified type
delete = delete all records of the specified type
help = shows this message

For "show" we have:

initial_date = date which the logs will start to be displayed

end_date = finish date to show the logs (dates must to be in the following format dd/mm/aaaa , if the date is not informed the log of the current day will be displayed)

priority = optional field. When provided, it must have one of the following values: ERROR, WARNING, NOTICE, INFORMATION, or DEBUG

(when selecting a priority, only the log which has the same priority informed will be informed)

Example 1: (showing logs from date 07/07/2003)

```
#fwlog show log 07/07/2003 07/07/2003

07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 of 0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 of 0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 of0
07/07/2003 19:06:22 (01) A TCP 10.4.1.24 1027 10.5.1.1 23 of 0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 of 0
07/07/2003 19:06:21 (01) A ICMP 10.5.1.134 10.4.1.12 8 of 1
07/07/2003 19:06:20 (01) A ICMP 10.4.1.12 137 10.5.1.134 0 of 0
07/07/2003 19:06:02 (01) A UDP 10.4.1.59 1050 10.7.1.25 53 of 0
```

Example 2: (showing logs from date 10/07/2003 to date 10/08/2003, only with debug priority level)

```
#fwlog show log 10/07/2003 10/08/2003 debug


07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 of 0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 of 0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 of 0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 of 0
```

Example 3: (erasing the log file)

```
#fwlog delete log 21/10/2003 23/10/2003

Removal of logs has been requested to the log server.
```

Viewing the system events

16. Viewing system events

This chapter will show how to view the system's events, it is a very useful resource to track firewall operation, and to detect possible attacks and configuration errors.

What are system events?

Events are high level firewall messages, i.e., those not directly related to packets (as logs are). In events, there may be messages generated by one of the three large modules (Packet Filter, Network Address Translator, and Authentication/Encryption), and also by any other firewall component, such as proxies and server processes in charge of specific tasks.

Basically, the type of information available varies from useful system tracking messages (generated, for example, every time the host is restarted, or every time a session is established with the firewall, etc.) to more critical configuration and execution error messages.

What is an event filter?

Despite being configured to record every possible event, the security system usually must provide, specific information, comparatively minute in volume (for example, all messages issued yesterday). The event filter is a mechanism offered by Aker Firewall to create logical views of the total set of event messages, facilitating access to the desired information.

Only information previously recorded in the events will be viewed through the filter. To obtain a certain type of information, it is necessary first to configure the system to record it, and then, use a filter to view it

16.1. Using the Remote Interface

To gain access to the events window follow the steps bellow:

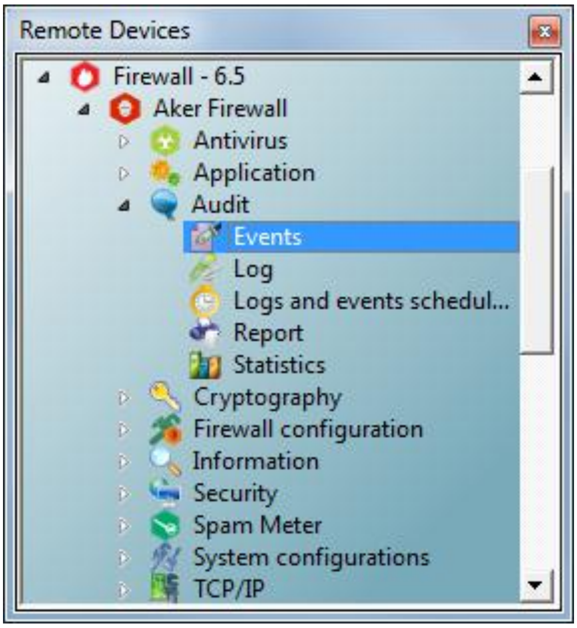

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Events
Log
Logs and events schedul...
Report
Statistics
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 330 – Access window: Events.

- Click on the menu *Audit*.
- Select the option *Events.*

Event toolbar

Every time the *Events* option is selected, its toolbar shows up. Located next to the other bars, it can be dragged and left floating on top of Events information. It has the following format:

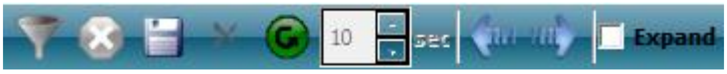
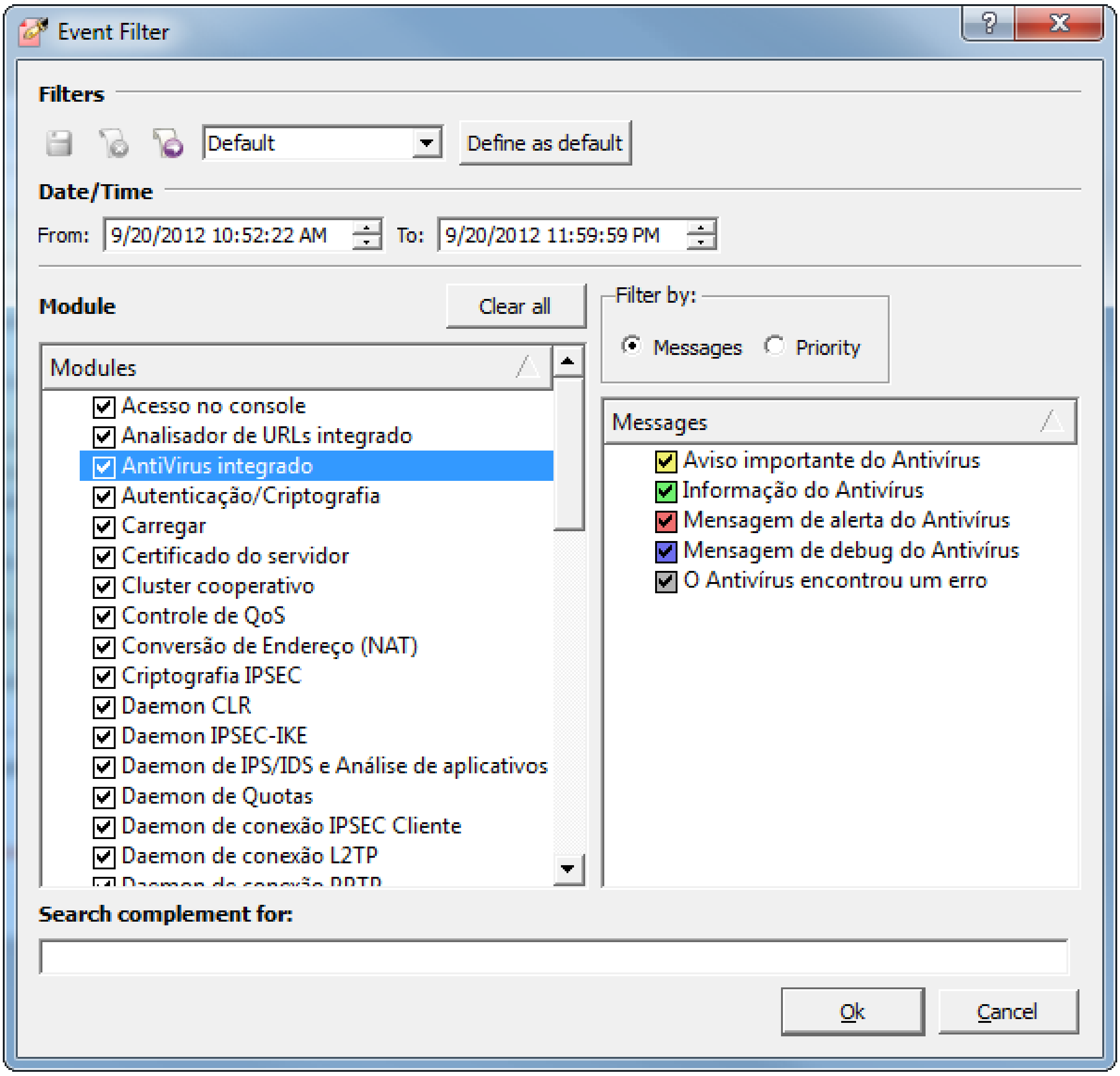

10
sec
Expand

Image 331 – Event toolbar.

Event Filter window



Filters: Default

From: 9/20/2012 10:52:22 AM To: 9/20/2012 11:59:59 PM

Filter by: ● Messages ○ Priority

Modules
- ☑ Acesso no console
- ☑ Analisador de URLs integrado
- ☑ AntiVirus integrado
- ☑ Autenticação/Criptografia
- ☑ Carregar
- ☑ Certificado do servidor
- ☑ Cluster cooperativo
- ☑ Controle de QoS
- ☑ Conversão de Endereço (NAT)
- ☑ Criptografia IPSEC
- ☑ Daemon CLR
- ☑ Daemon IPSEC-IKE
- ☑ Daemon de IPS/IDS e Análise de aplicativos
- ☑ Daemon de Quotas
- ☑ Daemon de conexão IPSEC Cliente
- ☑ Daemon de conexão L2TP

Messages
- ☑ Aviso importante do Antivírus
- ☑ Informação do Antivírus
- ☑ Mensagem de alerta do Antivírus
- ☑ Mensagem de debug do Antivírus
- ☑ O Antivírus encontrou um erro

Image 332 – Event filter.

The **Save**, **Remove**, and **New** buttons are located on the top part of the window. A new search filter may be saved, used later by the administrator, and removed when no longer needed.

To save an events filter, do the following:

1. Modify fields as needed.
2. Type in the name of the new filter in the **Filters** area.
3. Click on Save.

To apply a saved filter, select its name in the **Filters** area. All fields will be automatically filled with the saved data.

To delete a filter, do the following:

1. Select the filter to be removed in the **Filters** field.
2. Click on Remove.

The default filter is configured to show all messages of the current day. To change the preview to other days, you can configure the Initial ***date and*** the ***End date*** for the desired days.

In addition to the date criterion, it is also possible to filter messages to be displayed according to their generating module or by their Priority. In the **Filter** by option, you can choose between the Messages or the Priority lists.

Filter by messages

When the option Filter by Messages is selected, a list of all firewall modules is displayed on the left side of the window. When a module is selected, a list of all the different messages that module can generate is displayed on the right.

Hint: To select all messages of a module, click on the box on the left of the module name.

Filter by priority

Different types of messages have different priorities. The higher the priority of a record, the more important it is.

When the option Filter by Priority is selected, a list of all firewall modules is displayed on the left side of the window. When a module is selected, a list of all the different message priorities it may generate is displayed on the right.

All possible priorities, ordered by importance level, are explained below. (If the firewall is configured to send a copy of the events to the syslogd, the priorities with which the messages are generated in the syslog will be the same as below.)

- **Error**

  Records matching this priority level indicate some type of configuration or system operation error (insufficient memory, for example). Messages with this priority level are unusual and must be handled immediately.

- **Warning**

  Indicates some type of serious, atypical situation (remote user validation failure, for example).

- **Notice**

  Records with this priority level have information considered important to the system administrator, but are associated to routine situations (for example, an administrator initiated a remote session).

- **Information**

  These records add useful, although not vital, information to the Firewall administration (for example, the end of a remote administration session).

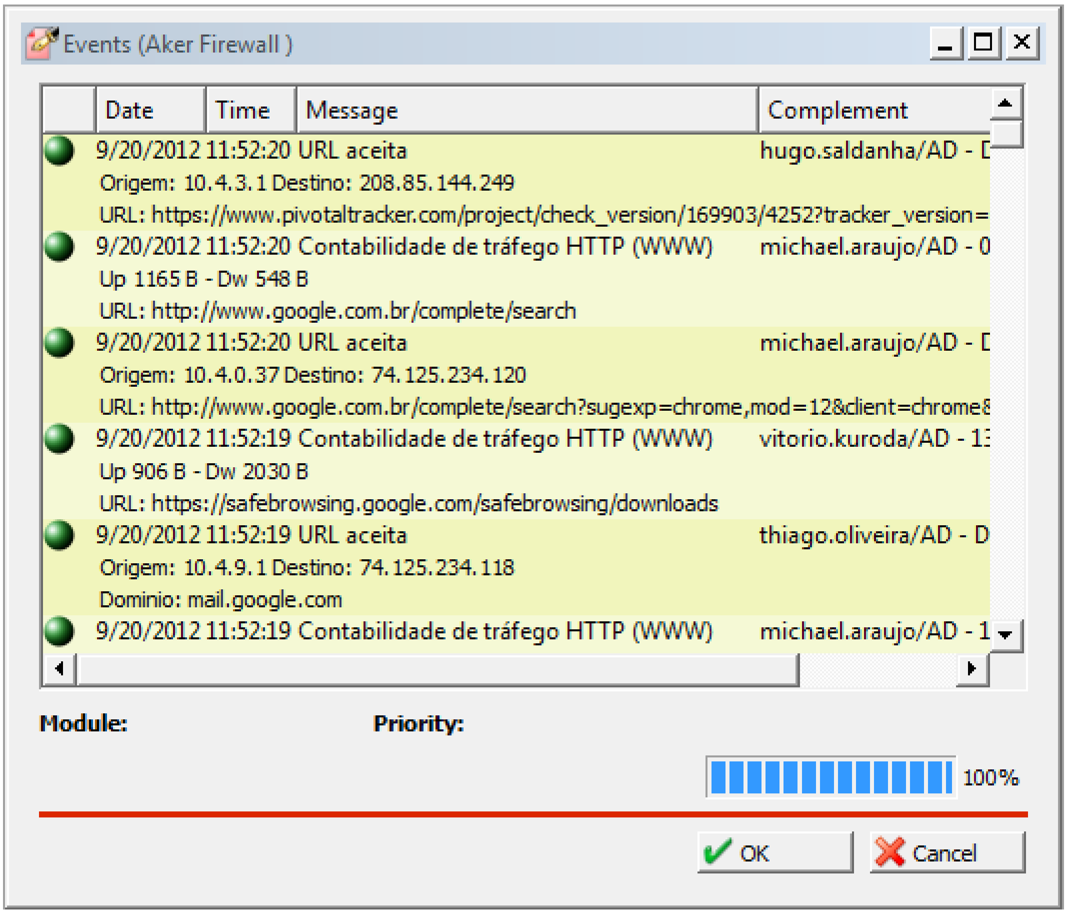
- **Debug**

  Records with this priority level have the least important information, except for audits. Examples of these types of messages are those generated by the remote administration module, every time the firewall configuration is modified, or when the firewall is reinitialized.

As a final filtering resource, there is the **field Search complement for**. It is used to specify a text that must be present in messages complements. Only messages complements containing this text will be displayed. This feature enables viewing all WWW (WORLD WIDE WEB) pages accessed by a certain user, just by inputting the user's name in this field.

- The **OK** button applies the chosen filter, and displays the Events Window with the selected information.
- The **Cancel** button cancels the filtering operation, and the Events Window is displayed with previous unmodified information.

Event window



```
Date      Time     Message                                        Complement
9/20/2012 11:52:20 URL aceita                                     hugo.saldanha/AD -
 Origem: 10.4.3.1 Destino: 208.85.144.249
 URL: https://www.pivotaltracker.com/project/check_version/169903/4252?tracker_version=
9/20/2012 11:52:20 Contabilidade de tráfego HTTP (WWW)            michael.araujo/AD - 0
 Up 1165 B - Dw 548 B
 URL: http://www.google.com.br/complete/search
9/20/2012 11:52:20 URL aceita                                     michael.araujo/AD -
 Origem: 10.4.0.37 Destino: 74.125.234.120
 URL: http://www.google.com.br/complete/search?sugexp=chrome,mod=12&client=chrome
9/20/2012 11:52:19 Contabilidade de tráfego HTTP (WWW)            vitorio.kuroda/AD - 1
 Up 906 B - Dw 2030 B
 URL: https://safebrowsing.google.com/safebrowsing/downloads
9/20/2012 11:52:19 URL aceita                                     thiago.oliveira/AD - D
 Origem: 10.4.9.1 Destino: 74.125.234.118
 Dominio: mail.google.com
9/20/2012 11:52:19 Contabilidade de tráfego HTTP (WWW)            michael.araujo/AD - 1
```

Image 333 – Description of events.

The Events Window is displayed after a new filter is applied. It has a list with several messages. Usually, each line corresponds to a different message however there may be messages with 2 or 3 lines. Message format will be explained in the next session.

Important observations:

- Messages will be displayed 100 at a time.
- Only the first 10,000 messages matching the chosen filter will be displayed. The remainder can be seen by exporting events to a file, or by using a filter that generates less events.
- To the left of each message, a colored icon will be displayed, representing its priority. Icon color legend is displayed below:

Blue	Debug
Verde	Information
Yellow	Notice
Red	Warning
Black	Error

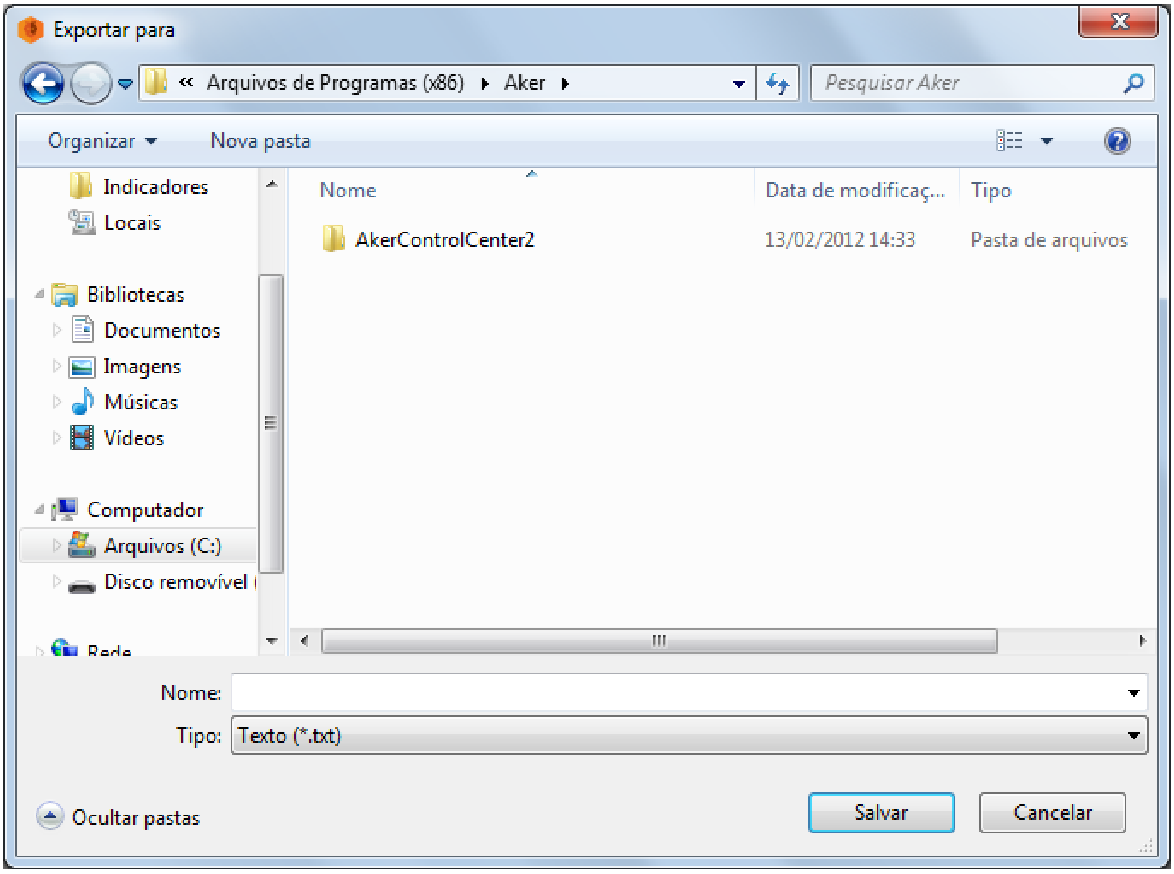
Additional information about a message can be obtained by clicking on it.

If all events are deleted, the only way to recover the information is restoring a backup copy.

- The **Save** button, located in the toolbar, saves all information selected by the current filter either in a text file format, or in formats that allow them to be imported by Aker and Web Trends (R) log analyzers. These files will have several lines of the same content displayed in the window

Events will be exported together with their additional messages if the *Expand* option is checked, and the option to export file of text type is chosen. Otherwise, the events will be exported without the messages.

This option is very useful when you want to send a copy of the log to someone else, to keep a text copy of important information, or to import a log by one of the log analyzers cited above. The following window will show up when the Export button is pressed.


Exportar para
« Arquivos de Programas (x86) ▸ Aker ▸
Pesquisar Aker
Organizar ▾
Nova pasta
Indicadores
Locais
Bibliotecas
Documentos
Imagens
Músicas
Vídeos
Computador
Arquivos (C:)
Disco removível (
Rede
Nome
Data de modificaç...
Tipo
Salvar
Cancelar
Ocultar pastas

Nome	Data de modificaç...	Tipo
AkerControlCenter2	13/02/2012 14:33	Pasta de arquivos

Nome:

Tipo: Texto (*.txt)

Image 334 – Exporting event logs.

To export the log content, name the file to be created, choose its type, and click on **Save**. To cancel the operation, click on **Cancel**.

In case there is already a file with the informed name it will be deleted.

- The **Next 100** button, represented by a right pointing arrow in the toolbar, shows the next 100 records selected by the filter. If there are no more records, this option is disabled.
- The **Previous 100** button, represented by a left pointing arrow in the toolbar, shows the previous 100 records. If there are no previous records, this option is disabled.
- The **Help** button shows specific help for the Log Window.

16.2. Format and meaning of messages and events fields

Below, there is a description of each message format, followed by a description of each of its fields. A complete list of all possible messages and their meanings can be found in Appendix A.

Record format

<Date> <Time> <Message> [Complement]
[Complementary message 1]
[Complementary message 2]

Fields description:

Date: Date that the record was generated.
Time: Time that the record was generated.
Message: Text message describing what happened.
Complement: This field contains additional information. It may or may not show up, depending on the message. In the Text Interface, if it shows up, it will be between parentheses.
Complementary message 1 and 2: These complements only exist in case of messages related to connections handled by transparent and non-transparent proxies. They are always displayed in the line below the main message. Complementary messages contain connection source address, and, in case of transparent proxies, the destination address

16.3. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action)*. All GUI functions are available, except for the message filtering option. Another limitation is that it is not possible, through the Text Interface, to access the additional information obtained when we select events message in the GUI, or when we activate the *Expand* option.

The software program that supports the events' Text Interface is the same one used with the log interface, and was also explained in the previous chapter.

Program location: /aker/bin/firewall/fwlog
Syntax:

```
Firewall Aker –
fwlog delete [log | log6 | events] [<initial_date> <end_date>]

fwlog show [log | events] [local | cluster] [<initial_date> < end_date>]
[priority]
```

Program help:

```
Usage: fwlog help
fwlog delete [log | log6 | events] [<initial_date> <end_date>]
fwlog show [log | log6 | events] [local | cluster] [<initial_date> <end_date>]
[priority]


fwlog – Text Interface used to view log and events
show = lists records of the specified type
delete = delete all records of the specified type
help = shows this message

For "show" we have:
initial_date = date which the logs will start to be displayed
end_date = finish date to show the logs (dates must to be in the dd/mm/aaaa
format, if the date is not informed the log of the current day will be displayed)
priority = optional field. When provided, it must have one of the following
values:  ERROR, WARNING, NOTICE, INFORMATION, or DEBUG

(When selecting a priority, only the log which has the same priority informed,
Will be informed)
```

Example 1: (showing events from date 10/07/2006 to date 10/08/2006)

```
#fwlog show events 10/07/2006 10/08/2006

10/08/2006 11:39:35 Administrative session closed
10/08/2006 09:13:09 Administrative session established (administrator, CF CL GU)
10/08/2006 09:13:09 Administrative session request (10.4.1.14)
10/08/2006 09:09:49 Operation on log file (Compact)
10/07/2006 10:27:11 Aker Firewall v6.0 – Initialization complete
10/07/2006 08:57:11 UDP translation table full
```

Example 2: (showing events from date 10/07/2006 to date 10/08/2006, only with debug priority level)

```
#fwlog show events 10/07/2006 10/08/2006 debug

10/08/2006 09:09:49 Operation on log file (Compact)
10/07/2006 10:27:11 Aker Firewall v5.0 – Initialization complete
```

Example 3: (erasing events file content)

```
#fwlog clear events 21/10/2006 23/10/2006

Records removal requested to log server.
```

Viewing statistics

17. Viewing statistics

In this chapter, we will explain the statistics of Aker Firewall and its characteristics.

What is the Aker Firewall Statistics Window?

In the Firewall, statistics are means of measuring data traffic through its interfaces. This traffic is translated into numbers that represent the total amount of packets sent or received, and the total number of bytes transported.

With this information, the administrator is able to relate data flow to each service, and he will know whether the network physical environment needs to be improved or expanded.

Network billing is another use for this type of information. Each network host is charged according to the amount of bytes they transfer.

To perform network billing, a filtering rule with a different counter for each host must be configured. Counters must have statistical rules associated to them. These rules are configured in the Statistics Window.

How Aker Firewall Statistics work?

The functioning of Aker Firewall statistics are based on three distinct steps:

- Creation of counters

  In this step, it is necessary to create the counters that will be associated with filtering rules. They serve only as totalizers for one or more filtering rules. For more information about the creation of counters and their association with filtering rules, refer to chapters ***Registering entities*** and ***Stateful inspection***.

- Creation of statistical rules

  After the creation of counters and their association with the desired filtering rules, it is necessary to create statistical rules that define the poll interval and which counters will be summed up to generate the value of the statistic on a given time. This step will be explained later on this chapter.

- Visualization of statistics

  After the creation of statistical rules, it is possible to view the values associated with any of the rules, export them or plot graphics. This step will also be explained on this chapter.

17.1. Using the Remote Interface

To gain access to the statistics configuration follow the steps bellow:

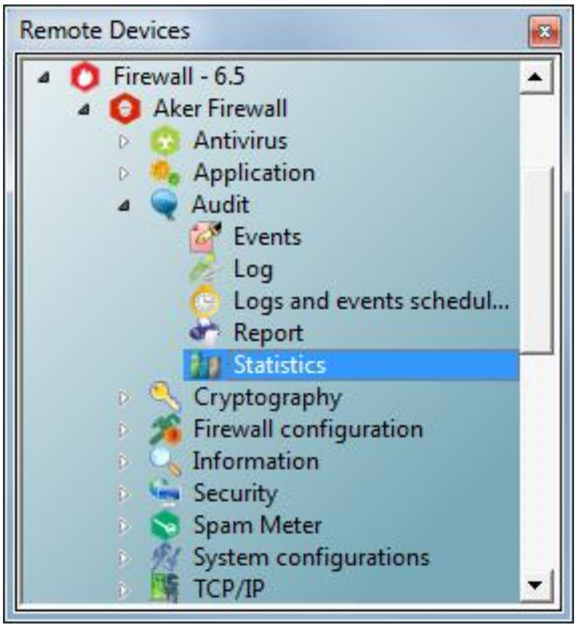
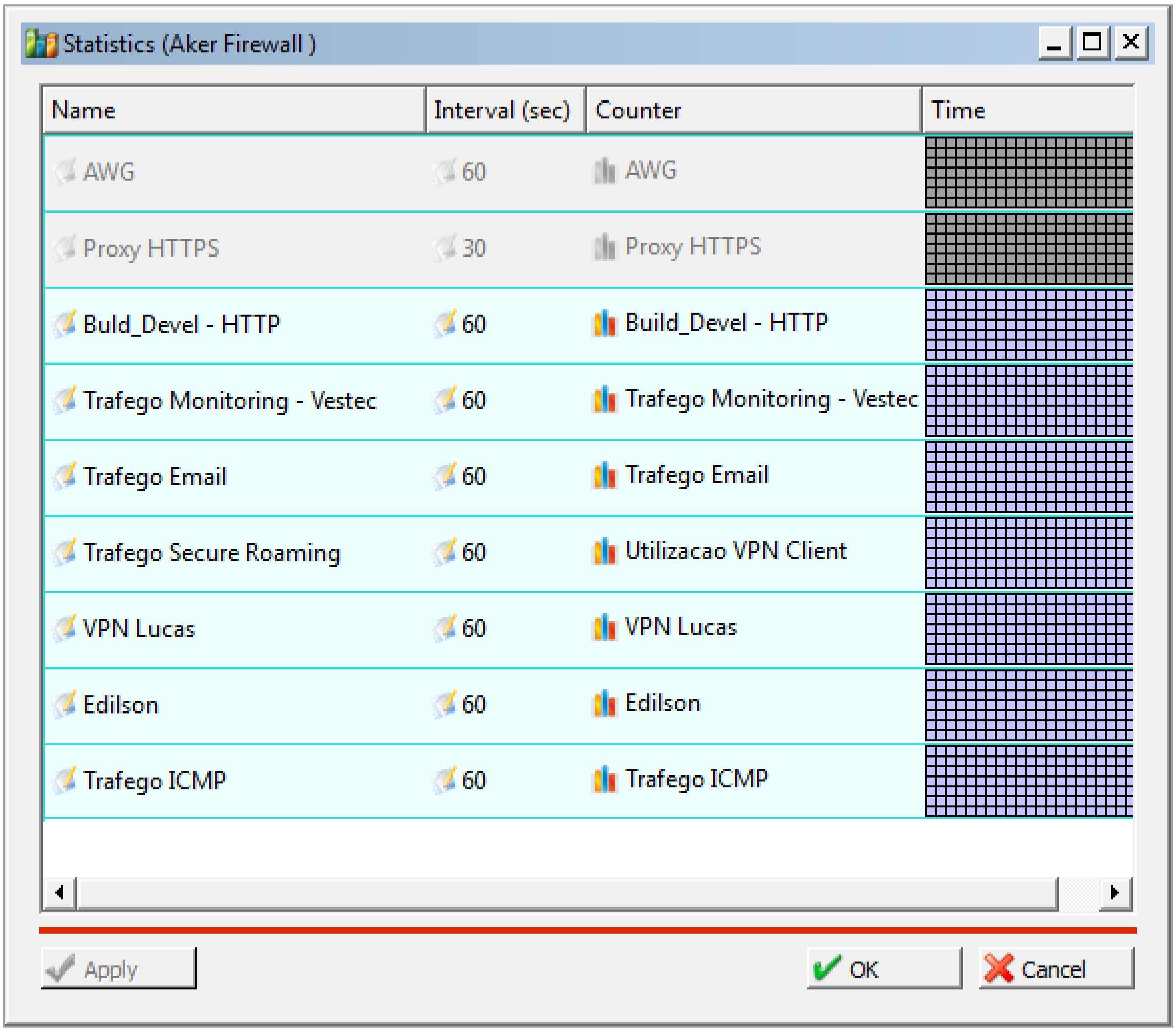

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Events
Log
Logs and events schedul...
Report
Statistics
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 335 – Event window – Statistics.

- Click on the menu *Audit*.
- Select *Statistics.*

Statistics window



Name	Interval (sec)	Counter	Time
AWG	60	AWG	
Proxy HTTPS	30	Proxy HTTPS	
Buld_Devel - HTTP	60	Build_Devel - HTTP	
Trafego Monitoring - Vestec	60	Trafego Monitoring - Vestec	
Trafego Email	60	Trafego Email	
Trafego Secure Roaming	60	Utilizacao VPN Client	
VPN Lucas	60	VPN Lucas	
Edilson	60	Edilson	
Trafego ICMP	60	Trafego ICMP	

Image 336 – Statistics rules.

The statistics window has all the statistical rules defined in Aker Firewall. Each rule is displayed in a separate row, made up of several cells. Selected rules are displayed on a different color.

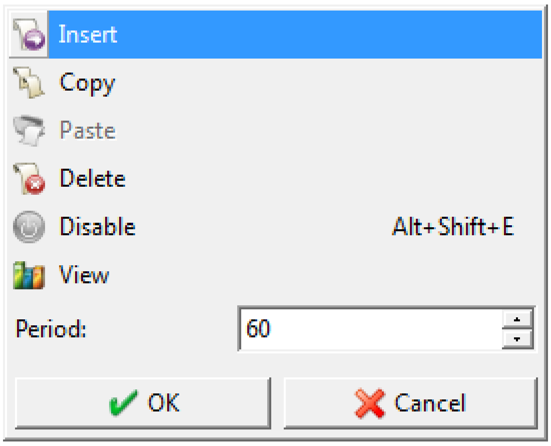
- The **OK** button updates the set of statistics and immediately enables them.
- The **Cancel** button discards all modifications and closes the window.
- The **Apply** button sends all modifications to the firewall and keep the window open
- The scrollbar to the right is used to view the rules that do not fit the window.

Each statistic rule is composed of the following fields:

- **Name:** Statistical rule name; to facilitate referencing. Each statistic rule must have a unique name within the rules set.
- **Interval:** Corresponds to the time interval that the totaling of rule will be made, i.e. the sum of the values of all counters present in the rule.

- **Counter:** This field establishes which counters will be summed up in this rule to generate the values of the rule.
- **Time:** This table defines date and time that the rule will be applicable. The lines represent weekdays, and columns represent the hours. To apply the rule at a specific time, check the box corresponding to it. Otherwise, leave it blank.

To interact with each rule, use the toolbar located on the top part of the window or right-click on it



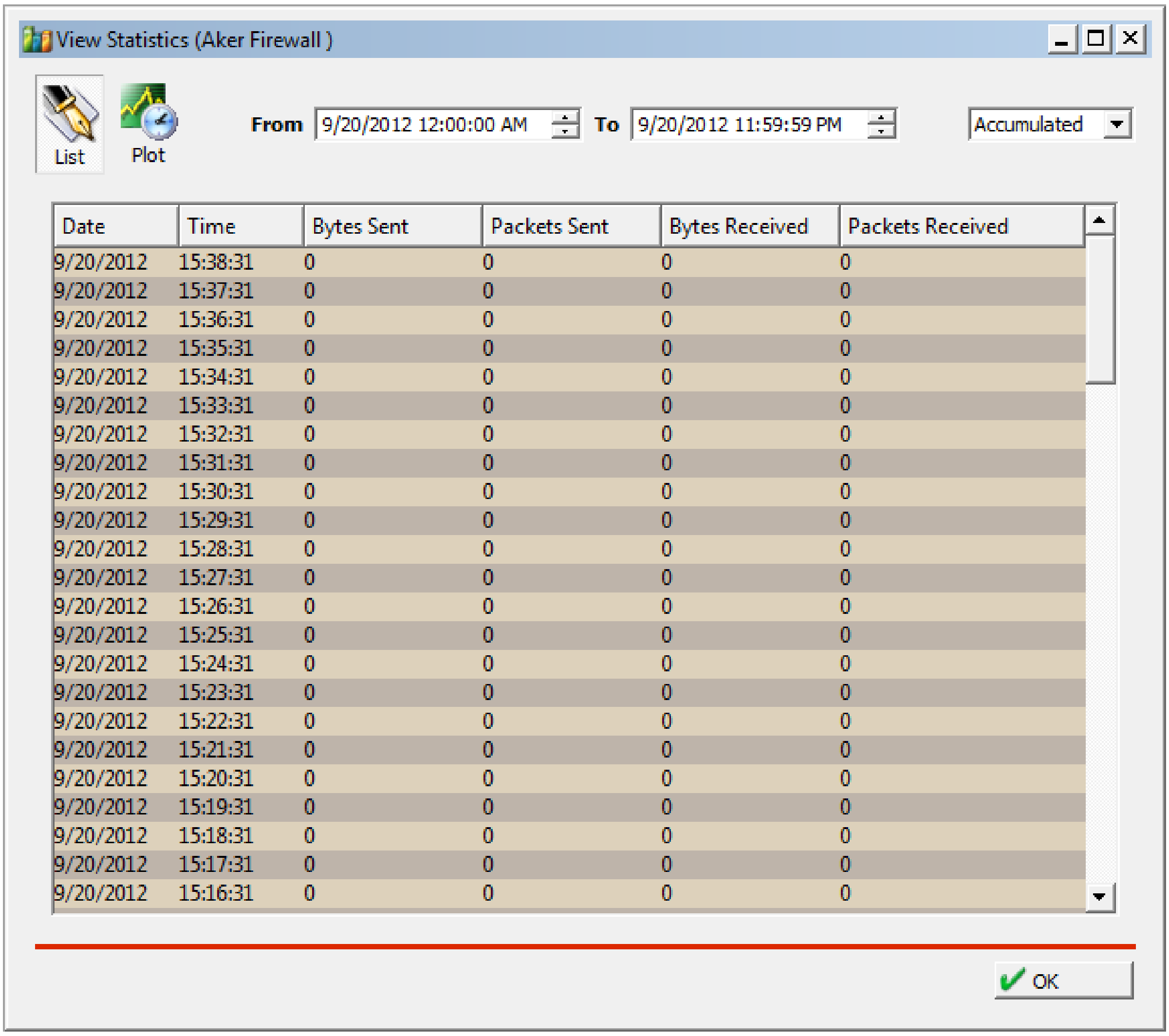
Period: 60

Image 337 – Statistics rules menu option.

- **Insert:** This option allows the addition of a new rule into the list.
- **Copy:** Removes the selected rule from the list.
- **Paste:** Copies the rule from the temporary area into the list. If any rule is already selected, the new one will be copied onto its position. Otherwise, it will be copied at the end of the list.
- **Enable/Disable:** Enables or disables the selected rule.
- **View:** Displays the view statistics window related to the selected rule.
- **Period:** It is the frequency that the statistics data will be collected, creating graphic and the lines in the table.

View statistics

When the **View** button is clicked or when a rule is double-clicked, the following window will be displayed:



From 9/20/2012 12:00:00 AM **To** 9/20/2012 11:59:59 PM Accumulated

Date	Time	Bytes Sent	Packets Sent	Bytes Received	Packets Received
9/20/2012	15:38:31	0	0	0	0
9/20/2012	15:37:31	0	0	0	0
9/20/2012	15:36:31	0	0	0	0
9/20/2012	15:35:31	0	0	0	0
9/20/2012	15:34:31	0	0	0	0
9/20/2012	15:33:31	0	0	0	0
9/20/2012	15:32:31	0	0	0	0
9/20/2012	15:31:31	0	0	0	0
9/20/2012	15:30:31	0	0	0	0
9/20/2012	15:29:31	0	0	0	0
9/20/2012	15:28:31	0	0	0	0
9/20/2012	15:27:31	0	0	0	0
9/20/2012	15:26:31	0	0	0	0
9/20/2012	15:25:31	0	0	0	0
9/20/2012	15:24:31	0	0	0	0
9/20/2012	15:23:31	0	0	0	0
9/20/2012	15:22:31	0	0	0	0
9/20/2012	15:21:31	0	0	0	0
9/20/2012	15:20:31	0	0	0	0
9/20/2012	15:19:31	0	0	0	0
9/20/2012	15:18:31	0	0	0	0
9/20/2012	15:17:31	0	0	0	0
9/20/2012	15:16:31	0	0	0	0

Image 338 – View statistics – List

In this window, the computed data for the statistics selected by user will be displayed in a graphic format:

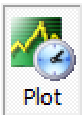


Image 339 – Button: Plot.

or text.

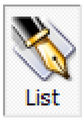


Image 340 – Button: List.

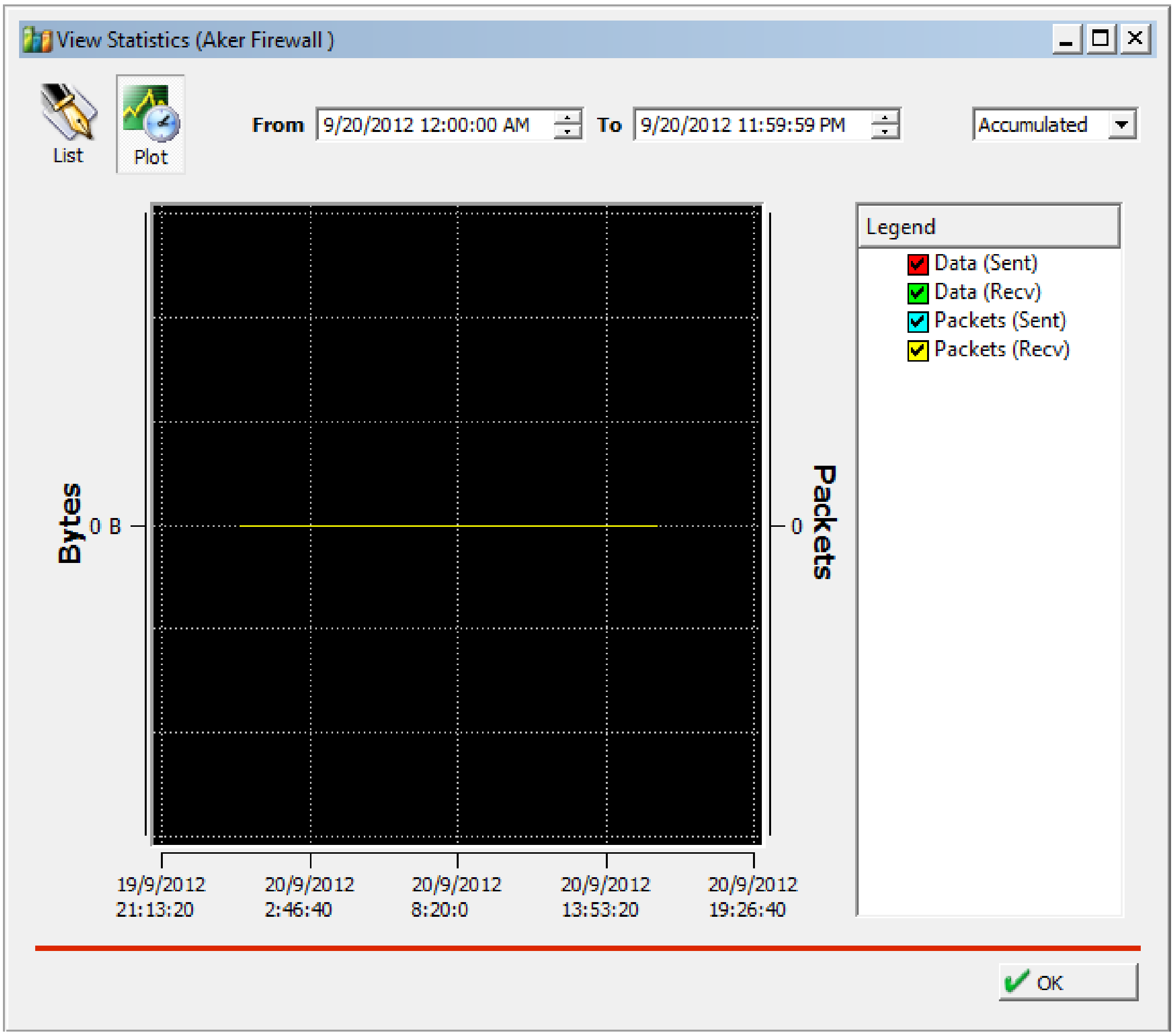
The information presented will correspond to a time period specified at the top. To alter it, select the **Date** field and input start/ending dates.

- **Reading:** Displays a set of 100 records at a time. Each record refers to the reconciling of counter stats during a specific time period.

  The **Remove** button deletes the set of records within the specified time period.

Image 341 – Button: remove.

Plot: Represents the **Reading** folder data in graphical format. Graphics are generated when this button is pressed. It allows the user to select which lines will be displayed, by pressing the legend buttons.



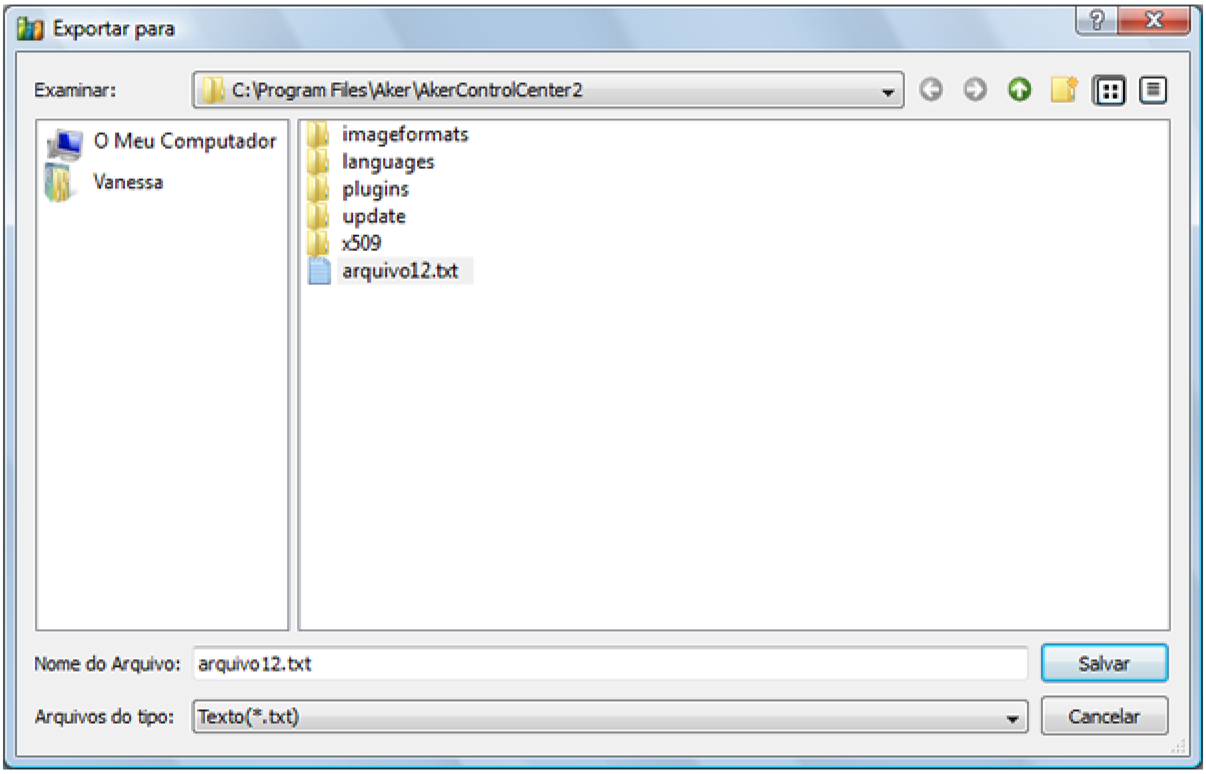
View Statistics (Aker Firewall)
List
Plot
Bytes
0 B
0
Packets
19/9/2012 21:13:20
20/9/2012 2:46:40
20/9/2012 8:20:0
20/9/2012 13:53:20
20/9/2012 19:26:40
Legend
☑ Data (Sent)
☑ Data (Recv)
☑ Packets (Sent)
☑ Packets (Recv)
OK

From 9/20/2012 12:00:00 AM **To** 9/20/2012 11:59:59 PM Accumulated

Image 342 –View statistics – Plot.

When the Save Statistics button is pressed the following window is displayed. This file is recorded in CSV format, enabling manipulation through spreadsheet programs.

Image 343 – Button: save statistics.



Exportar para
O Meu Computador
Vanessa
imageformats
languages
plugins
update
x509
arquivo12.txt
Salvar
Cancelar

Examinar: C:\Program Files\Aker\AkerControlCenter2

Nome do Arquivo: arquivo12.txt

Arquivos do tipo: Texto(*.txt)

Image 344 – Exporting statistics.

View statistics toolbar

The view statistics toolbar has the following functions:

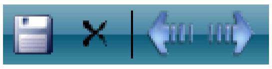


Image 345 – toolbar: view statistics.

17.2. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command* *“fwshell” before you take any action).* All functions are available, except for graphical data verification, as well as, which and where are the rules included in a counter.

To view the timetable do the following:

The : (colon) indicates that the rule is valid for both weekdays that appear separated by a slash (/). For example: Sun/Mon.
The . (period) indicates that rule is only valid for the weekday written after the slash (/). In the above example, Sun/Mon, it would be valid for Monday only.
The ' (apostrophe), or single quotes, indicates that the rule is only valid for the weekday written before the slash (/). This way, in Sun/Mon, it would be valid for Sunday only.

Program location: /aker/bin/firewall/fwstat

Syntax:

```
fwstat help
      show [[-c] <statistic> [<initial date> <final date>]]
      include <statistic> <period> [<counter1> [counter2] ...]
      remove <statistic>
      disable <statistic> [<day> <hour>]
      enable <statistic> [<day> <hour>]
```

Program Help:

```
Aker Firewall –

Usage: fwstat help
            show [[-c] <statistic> [<initial date> <final date>]]
            include <statistic> <period> [<counter1> [counter2] ...]
            remove <statistic>
            disable <statistic> [<day> <hour>]
            enable <statistic> [<day> <hour>]

      help      = shows this message
      show      = with no parameters, shows the collected data of the registered
statistics
      statistic = statistic name
      -c        = outputs in CSV (comma separated value) format
                  (Useful to import data in spreadsheets)
      dates     = boundary dates for statistic output
      include   = adds a new statistic named "statistic"
      remove    = removes a statistic named "statistic"
      period    = data collection period (seconds)
      counter = name of the counter entities to collect
```

disable = disables a statistic
enable = enables a statistic
day, hour = if specified (always both) enables or disables only for the specified time. 'day' belongs to {sun, mon, tue, ...} and 'hour' to {0.23}

Example 1: (showing statistics)

```
#fwstat show
Name  : statistics1                              (enabled)
----
Period : 17400 seconds (s)
Counters: a1
Time:
Day\Time|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
-------------------------------------------------------------------------------
Sun/Mon |:  :                    :  :  :  :  :  :  :  :  :  :  :  :  :  :
Tue/Wed |:  :                    :  :  :  :  :  :  :  :  :  :  :  :  :  :
Thu/Fri |:  :                 :  :  :  :  :  :  :  :  :  :  :  :  :  :
Sat     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '

Name  : statistics2                              (enabled)
----
Period  : 100  seconds(s)
Counters: a1  a11
Time:
Day\Time|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
-------------------------------------------------------------------------------
Sun/Mon |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
Tue/Wed |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
Thu/Fri |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
Sat     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '    ,    '
```

Example 2: (showing statistics from date 10/28/2001 to date 10/29/2001)

```
#fwstat show statistics 10/28/2001 10/29/2001
Day          Time       Sent (bytes/packets)      Received (bytes/packets)
----------------------------------------------------------------------
10/29/2001 17:24:54         320/1                    321/1
10/29/2001 17:23:14         652/6                    654/6
10/29/2001 17:21:34         234/2                    980/9
10/29/2001 17:19:54         324/3                    650/6
10/29/2001 17:18:14         325/3                    150/1
10/29/2001 17:16:34         985/9                    240/2
10/29/2001 17:14:54         842/8                    840/8
10/29/2001 17:13:14         357/3                    289/2
```

10/29/2001 16:58:14	786/7	261/2

Viewing and removing connections

18. Viewing and removing connections

In this chapter will be displayed how to view and remove the TCP connections and UDP session in real-time.

What are active connections?

Active connections are TCP connections or UDP sessions which are active through the Firewall. Each one of these connections has been validated through a stateful filter rule, which has been added by the system administrator, or through an entry in the state table, automatically added by Aker Firewall.

For each of these connections, the firewall keeps a lot of information in its state tables. Some of these pieces of information are especially useful to the administrator and they can be viewed at any moment through the active connections window. This information contains the exact hour of establishment of the connections and their idle time, i.e., the amount of time that no packets have passed through them.

18.1. Using the Remote Interface

To gain access to the connections window follow the steps bellow:

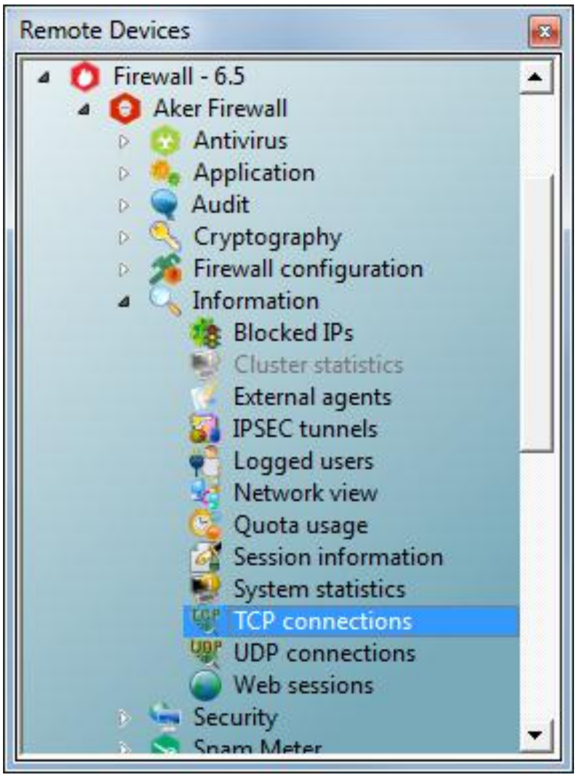

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter

Image 346 – Access window: TCP connection.

- Click on the menu *Information*
- Select *TCP connections or UDP connections.*

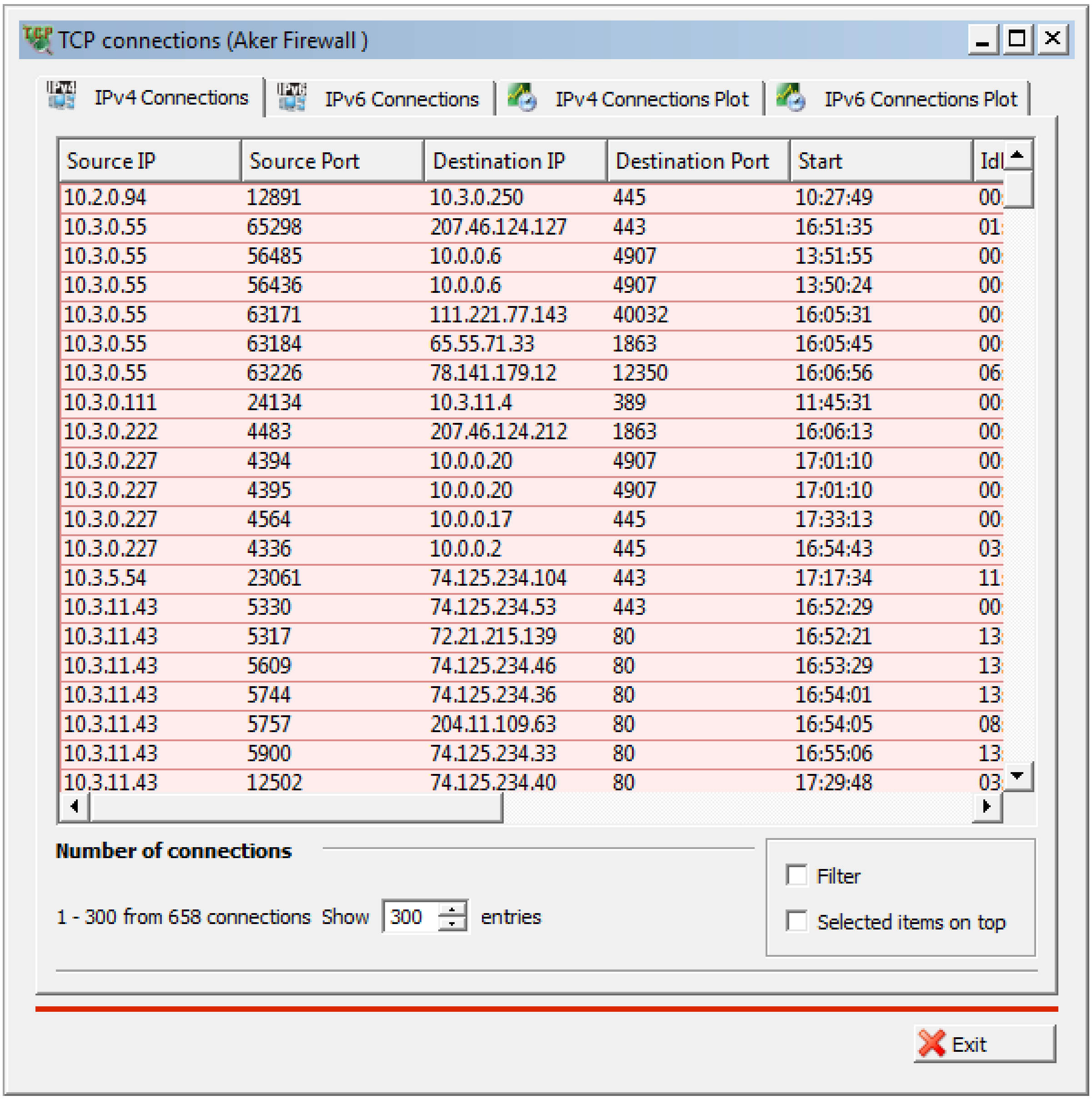
The active connections window

The active connections window is where all the connections that are running through the firewall, during a specific moment, can be viewed. The windows for the TCP and UDP protocols are identical, except for the field called **Current State,** which only exists in the TCP connections window.

In order to simplify the understanding, TCP and UDP connections are often mentioned; however, this feature is not real due to the fact that the UDP protocol is not connection oriented. In fact, the meaning of the UDP connection term is an UDP session where a two-way traffic takes place. Each session can be seen as a set of request and response packets which go through the firewall to a specific service, provided by one host and accessed by another.

This window consists of two tabs: the first tab shows a list with the active connections and the second tab displays a real-time graphic with the most used hosts and services

IPv4 connections



Source IP	Source Port	Destination IP	Destination Port	Start	Idl
10.2.0.94	12891	10.3.0.250	445	10:27:49	00:
10.3.0.55	65298	207.46.124.127	443	16:51:35	01:
10.3.0.55	56485	10.0.0.6	4907	13:51:55	00:
10.3.0.55	56436	10.0.0.6	4907	13:50:24	00:
10.3.0.55	63171	111.221.77.143	40032	16:05:31	00:
10.3.0.55	63184	65.55.71.33	1863	16:05:45	00:
10.3.0.55	63226	78.141.179.12	12350	16:06:56	06:
10.3.0.111	24134	10.3.11.4	389	11:45:31	00:
10.3.0.222	4483	207.46.124.212	1863	16:06:13	00:
10.3.0.227	4394	10.0.0.20	4907	17:01:10	00:
10.3.0.227	4395	10.0.0.20	4907	17:01:10	00:
10.3.0.227	4564	10.0.0.17	445	17:33:13	00:
10.3.0.227	4336	10.0.0.2	445	16:54:43	03:
10.3.5.54	23061	74.125.234.104	443	17:17:34	11:
10.3.11.43	5330	74.125.234.53	443	16:52:29	00:
10.3.11.43	5317	72.21.215.139	80	16:52:21	13:
10.3.11.43	5609	74.125.234.46	80	16:53:29	13:
10.3.11.43	5744	74.125.234.36	80	16:54:01	13:
10.3.11.43	5757	204.11.109.63	80	16:54:05	08:
10.3.11.43	5900	74.125.234.33	80	16:55:06	13:
10.3.11.43	12502	74.125.234.40	80	17:29:48	03:

Number of connections

1 - 300 from 658 connections Show 300 entries

☐ Filter

☐ Selected items on top

Image 347 – TCP connections –IPv4 connections.

IPV6 connections

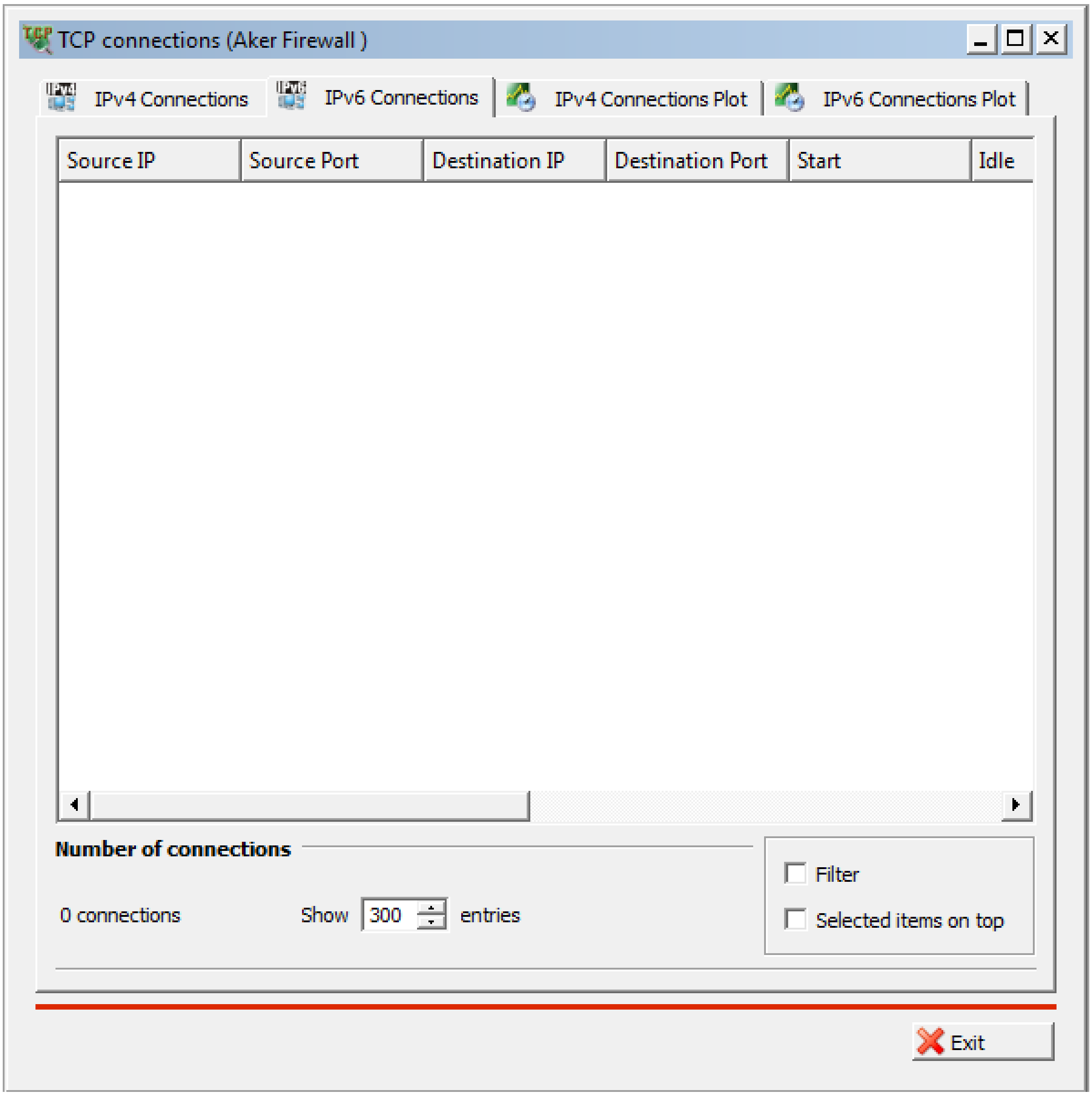

TCP connections (Aker Firewall)
IPv4 Connections
IPv6 Connections
IPv4 Connections Plot
IPv6 Connections Plot
Source IP
Source Port
Destination IP
Destination Port
Start
Idle
Number of connections
0 connections
Show 300 entries
☐ Filter
☐ Selected items on top
Exit

Image 348 – TCP connections – IPv6 connections.

IPv4 and IPv6 connections tabs consist of a list with an entry for each active connection. A message with the total number of active connections at a specific moment is displayed at the bottom of the window.

- The **OK** button will close the active connections window.
- The **Filter** option shows the filtering options, enabling the selection of source or destination addresses and/or ports to be displayed in the window.
- The **Selected items on top** option displays the selected connections on the top of the window, for better visualization

- The **Delete** option, displayed when the right mouse button is clicked on a connection, will remove the selected connection.
-

When a TCP connection is removed, the firewall sends reset packets to the hosts which are taking part in the connection, effectively dropping it, and removes the entry from its state table. In case of UDP connections, the firewall simply removes the entries from its state table, prohibiting then, the acceptance of packets to the removed connections.

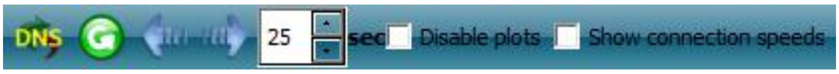


Image 349 – TCP connections toolbar.

All made changes on the toolbar, when the IPv4 connection or IPv4 graphic options are selected, will be performed as well on the IPv6 connection or IPv6 graphic options, and so on.

- The **Refresh** button, located on the toolbar, will activate (or deactivate) the automatic refresh of the displayed information, which is enabled by default. The first time this button is clicked, the automatic refresh will be deactivated. To reactivate it, just click on it again. The refresh interval can be configured by changing the value on the right of this button.

- The **DNS** button, located on the toolbar, will trigger the domain name system (DNS) to resolve the names of the hosts whose IP addresses are listed. The following should be mentioned:

  1. The name resolution is very often a slow service, and because of this trait, the resolution is performed in the background.
  2. Many times, due to reverse DNS configuration problems (which is used to resolve names from IP addresses), the resolution of certain addresses will not be possible. In such case, the addresses which have not been resolved will be kept in their original form and it will be indicated, besides them, that they do not have a reverse DNS configured.

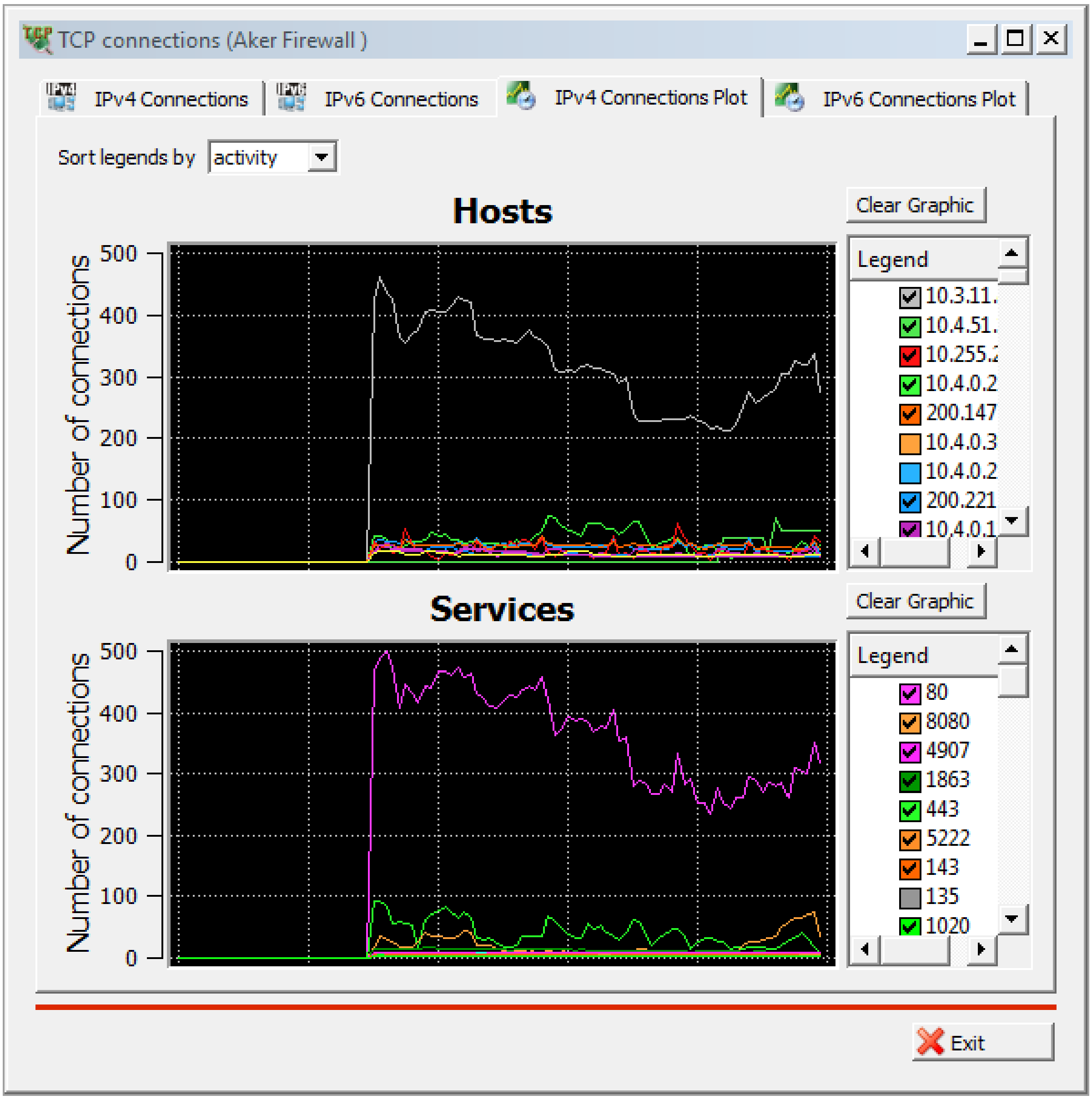
- The **Disable plots** option disables the plotting of the connections graphic and it is useful for slow speed computers

- The **Show connection speeds** option, if enabled, causes the interface to calculate and show each connection speed in bits/s.

- It is possible to sort the connection list by any of its fields, being just necessary to click on the field title. The first click will generate an ascending sort and the second will reverse the list.

IPv4 e IPv6 connections plot

The IPv4 and IPv6 plot tab consists of two graphics: the upper one shows the most used services and the lower one shows the most accessed hosts. In the right side there is a caption showing which host or service corresponds to which graphic color.


TCP connections (Aker Firewall)
IPv4 Connections
IPv6 Connections
IPv4 Connections Plot
IPv6 Connections Plot
Hosts
Clear Graphic
Number of connections
500
400
300
200
100
0
Legend
☑ 10.3.11.
☑ 10.4.51.
☑ 10.255.2
☑ 10.4.0.2
☑ 200.147
☐ 10.4.0.3
☐ 10.4.0.2
☑ 200.221
☑ 10.4.0.1
Services
Clear Graphic
Number of connections
500
400
300
200
100
0
Legend
☑ 80
☑ 8080
☑ 4907
☑ 1863
☑ 443
☑ 5222
☑ 143
☐ 135
☑ 1020
Exit

Sort legends by activity

Image 350 – TCP connections –IPv4 connections Plot.

The time interval which the plot is updated and the same configured in the connections tab.

Meaning of fields of an IPv6 and IPv4 *active connection*

Each line of the active connections list represents one connection. The meaning of its fields is the following:

Source IP: IP address of the host which initiated the connection.

Source port: Port used by the source host to establish the connection.

Destination: IP address of the host which the connection was established to.

Destination port: Port which the connection has been established to. This port is usually associated with a specific service.

Start: Connection establishment time.

Idle: Number of minutes and seconds the connection is idle.

Status: This field is displayed only in case of TCP connections. It represents the connection state at the moment it is displayed. It can have the following values:

> **SYN Sent:** It indicates that the connection request packet (packet with the SYN flag) has been sent, however, the server has not responded yet.
>
> **SYN Exchanged:** It indicates that the connection request packet has been sent and the server has responded with a confirmation that the connection has been accepted.
>
> **Established:** It indicates that the connection is established.
>
> **Listening at port:** Indicates that the server is listening at the indicated port waiting for a connection from the client. This state only occurs for FTP data connections.

Bytes sent/received: These fields appear only in case of TCP connections and indicate the amount of bytes that passed through a connection in both directions.

Packets sent/received: These fields appear only in case of TCP connections and indicate the number of packets that passed through a connection in both directions

18.2. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action)*. The same program deals with both TCP and UDP connections.

Program location: /aker/bin/firewall/fwlist

Syntax:

```
Usage: fwlist help
fwlist show [[-w] [TCP]] | [UDP] | [session]
fwlist remove [TCP | UDP] source_IP source_Port destination_IP destination_Port
fwlist remove session source_IP
```

Program help:

```
fwlist – Lists and removes TCP/UDP connections and  active sessions

Usage: fwlist help

    fwlist show [[-w] [TCP | TCP6]] | [UDP | UDP6]

    fwlist show [sessions | roaming | blocked]

    fwlist show [quotas | www]

    fwlist remove [TCP | TCP6 | UDP | UDP6] source_IP source_Port

                destination_IP destination_Port

    fwlist remove sessions source_IP [user]

    fwlist remove blocked source_IP

    fwlist restart [ user <name> ] [ quota <name> ] [time] [volume]


    help    = shows this message

    show    = lists active connections or sessions

    remove    = removes an active connection or session

    restart = restarts users quota
```

Example 1: (listing the TCP active connections)

```
#fwlist show TCP

Source(IP:port)     Destination(IP:port)  Start    Idle    State
-------------------------------------------------------------------------
```

```
10.4.1.196:1067     10.4.1.11:23        15:35:19 00:00   Established
10.4.1.212:1078     10.5.2.1:25         15:36:20 00:10   Established
```

Example 2: (listing the UDP active connections)

```
#fwlist show UDP
```

```
Source(IP:port)     Destination(IP:port)  Start    Idle
---------------------------------------------------------
10.4.1.1:1099       10.4.1.11:53        15:35:19 00:00
10.4.1.18:1182      10.5.2.1:111        15:36:20 00:10
```

Example 3: (removing a TCP connection and listing the connections)

```
#fwlist remove tcp 10.4.1.196 1067 10.4.1.11 23
```

```
#fwlist show TCP
```

```
Source(IP:port)     Destination(IP:port)  Start    Idle    State
-----------------------------------------------------------------------
10.4.1.212:1078     10.5.2.1:25         15:36:20 00:10   Established
```

Using the reports generator

19. Using the Reports generator

This chapter will show what is for and how to configure the Reports in Aker Firewall.

This tool was developed to provide information through the data present in the log and events records, giving a summarized view for the Firewall management.

The records are generated in HTML, TXT or PDF format, published via FTP in up to three distinct web sites or sent through e-mail for three distinct recipients at maximum. It can be scheduled in the following ways: "Daily", "Weekly", "Semimonthly", "Monthly", "Specific" and the option *generate daily report now*.

19.1. Accessing reports

To gain access to the report window follow the steps bellow:

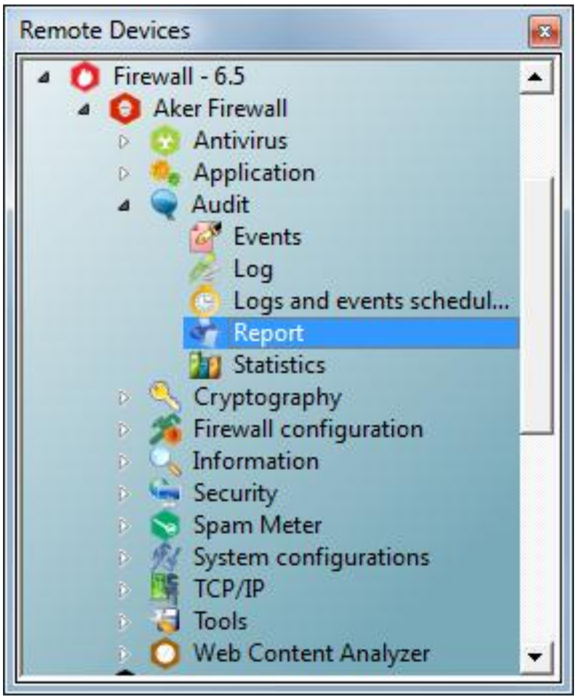
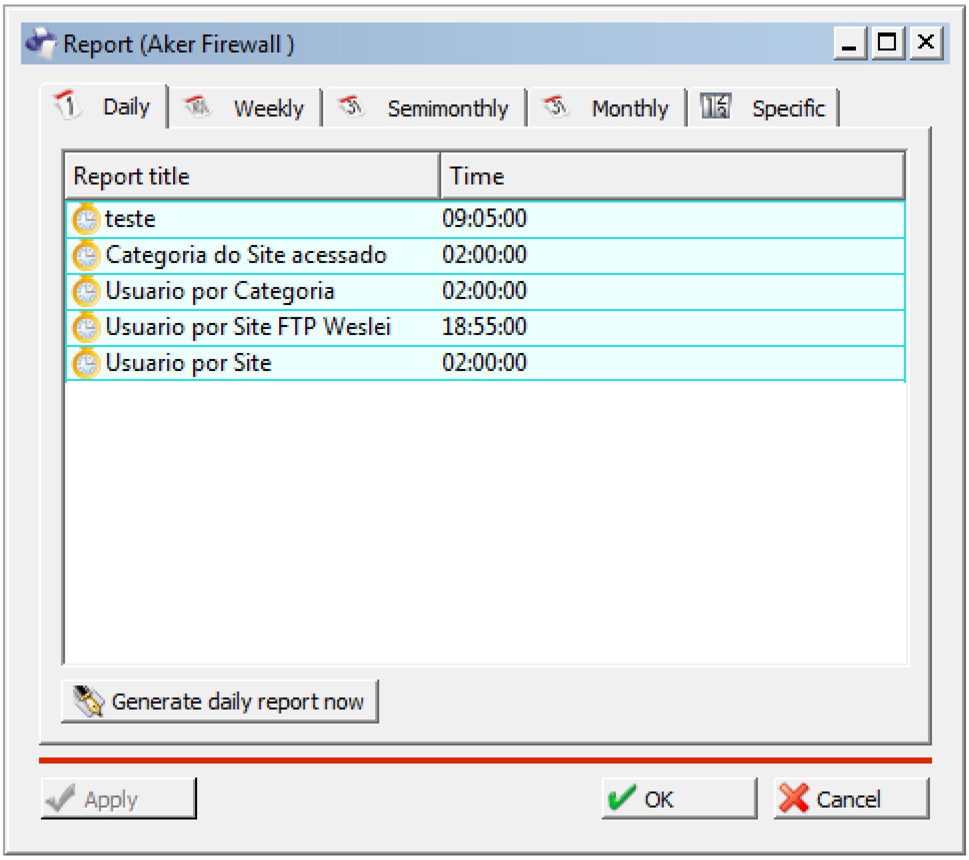

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Events
Log
Logs and events schedul...
Report
Statistics
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 351 – Access window: Report.

- Click on the *Audit menu*.
- Select *Report*.

19.2. Configuring Reports


Report (Aker Firewall)
Daily
Weekly
Semimonthly
Monthly
Specific
Generate daily report now
Apply
OK
Cancel

Report title	Time
teste	09:05:00
Categoria do Site acessado	02:00:00
Usuario por Categoria	02:00:00
Usuario por Site FTP Weslei	18:55:00
Usuario por Site	02:00:00

Image 352 – Configuring reports – Daily.

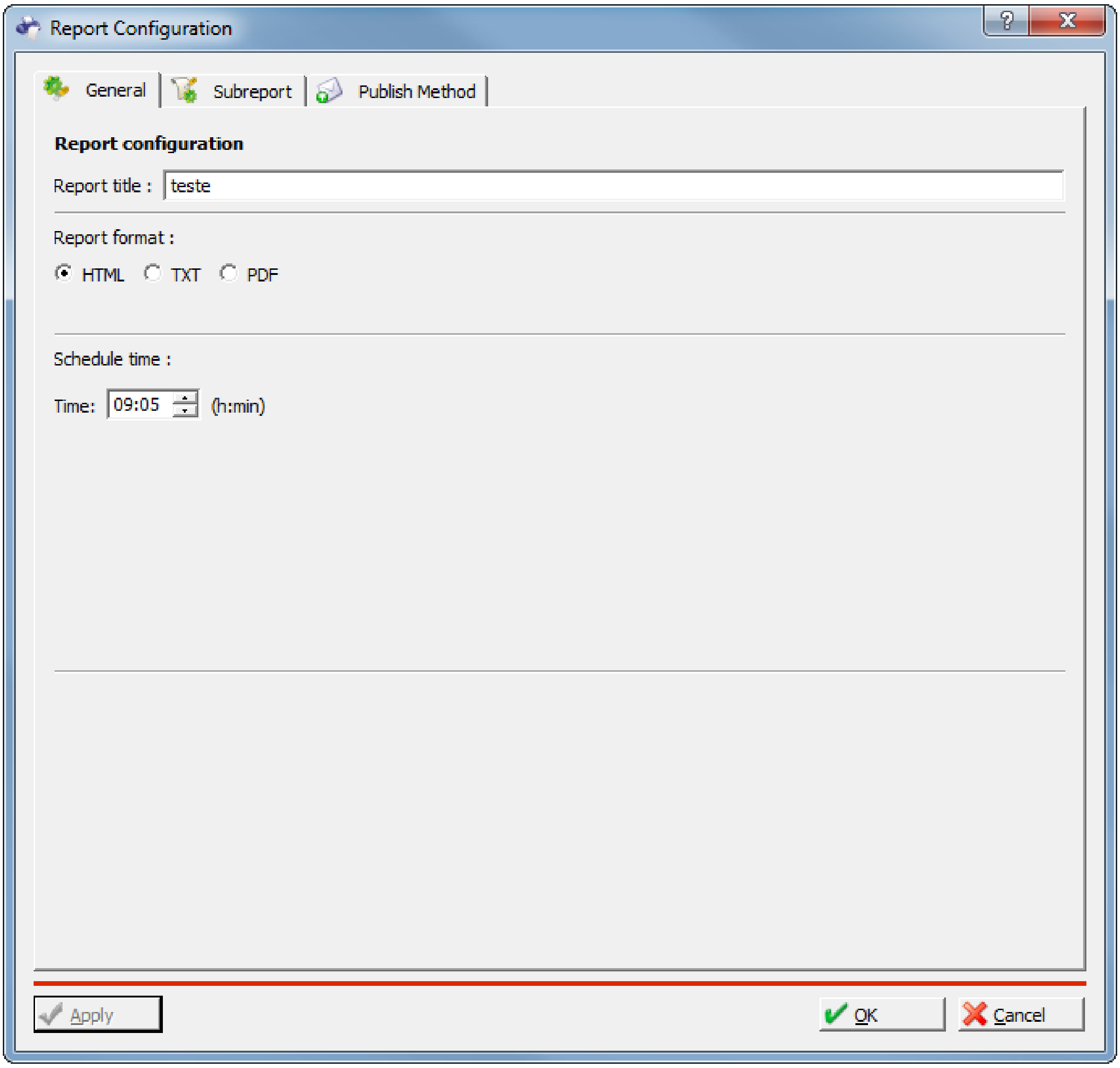
This window is composed by the following types of schedules: "Daily", "Weekly", "Semimonthly", "Monthly", "Specific" and the option “*generate daily report now”*. In all of them will be necessary to choose which subreport will be included.

In order to execute any report, you have to right-click on the report or double click on it. Then the window bellow will be displayed (in case no report is selected you will have only the option *Insert).*

- **Insert:** This option includes a new report.

When inserting a new report two tabs shall be presented, the description of them follows bellow:

General tab


Report Configuration
General
Subreport
Publish Method
Apply
OK
Cancel

Report configuration

Report title : teste

Report format :

● HTML ○ TXT ○ PDF

Schedule time :

Time: 09:05 (h:min)

Image 353 – Report configuration- general.

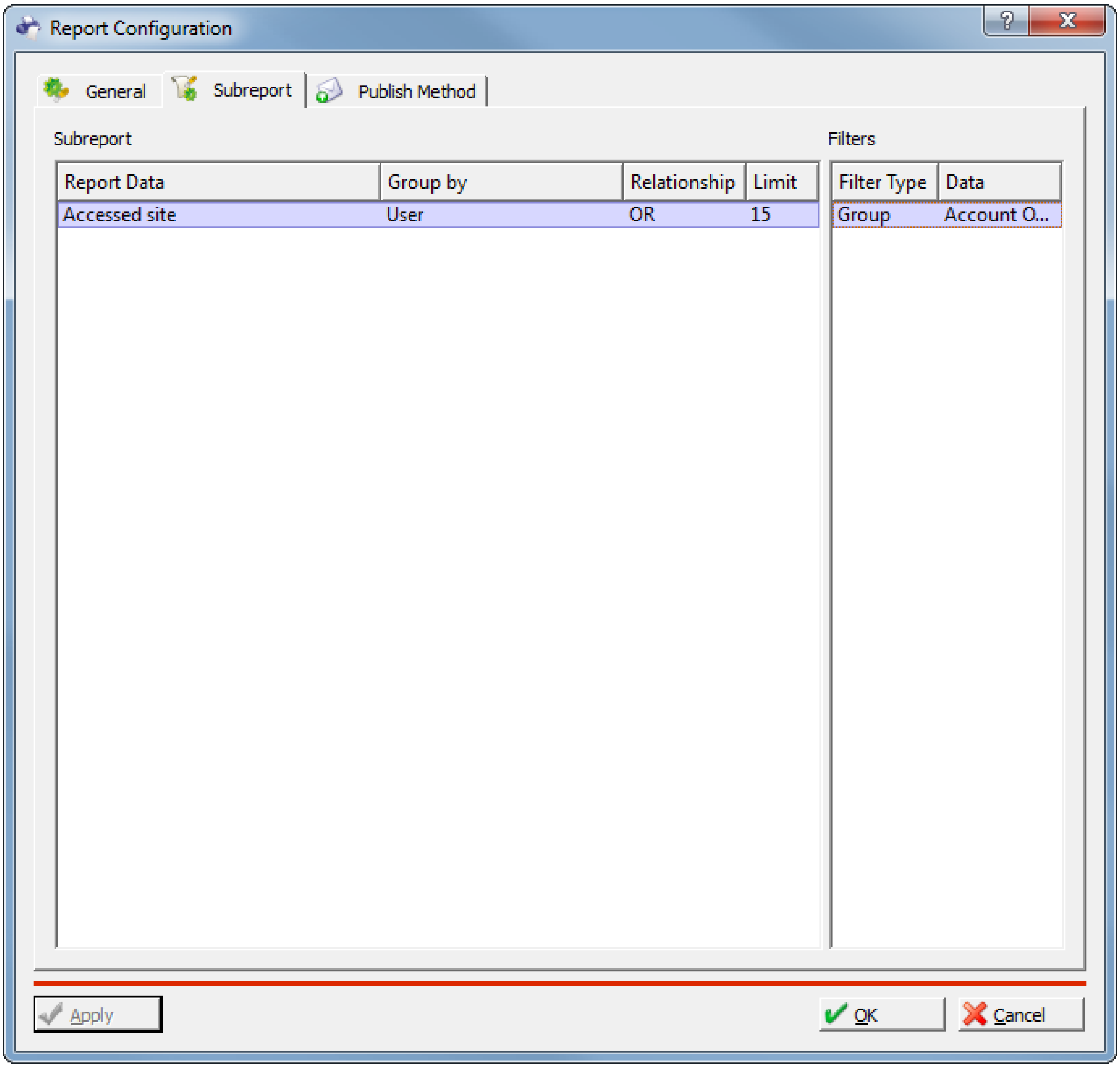
- **Report title:** Assigns a name to the report.
- **Schedule time:** Defines the time that the report will be generated.
- **Report format**: Defines the format that the report will be generated. The format options are:

  - **TXT:** When this option is selected a file called report.txt containing the report will be generated.
  - **HTML**: When this option is selected a file called index.html containing the report will be generated.
  -
  - **PDF**: When this option is selected a file called report.pdf containing the report will be generated.

In both cases the browser will be opened automatically, showing the content corresponding to its report.

Subreport tab

A subreport is offered so the detail levels can be evidenced and the information that composes the report becomes more objective.



Subreport

Report Data	Group by	Relationship	Limit
Accessed site	User	OR	15

Filters

Filter Type	Data
Group	Account O...

Image 354 – Report configuration – Subreport.

This tab consists of two columns, where will be necessary to indicate the filters.

In the **"Subreport tab"** the Subreport type must to be included and how it will be grouped, for example: "Do not group", "Quota", "User". This option may vary depending on the type of Subreport. It is possible to define the relationships with logic “E” or “OR” and a limit for TOP.

In the **"Filters"** column you will have more options according to the given *Filter Type*.

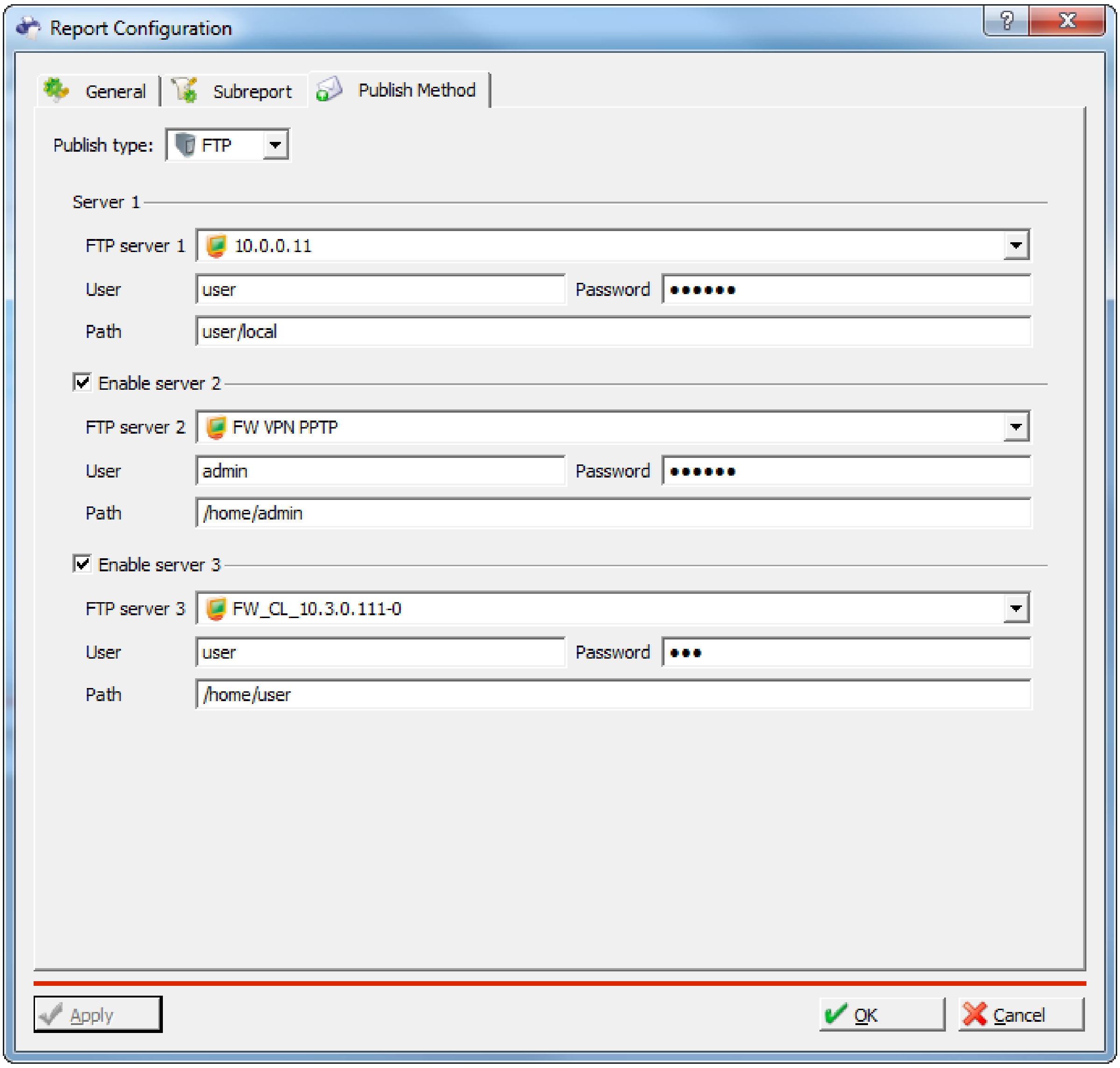
Publish Method

FTP Method

In this tab the user will be able to indicate up to three servers where the reports will be sent via FFTP.

How to use:

- Select the server or servers;
- Type the user;
- Type the password;
- Type the path of the report destination.


Report Configuration
General
Subreport
Publish Method
Apply
OK
Cancel

Publish type: FTP

Server 1

FTP server 1: 10.0.0.11

User: user Password: ••••••

Path: user/local

☑ Enable server 2

FTP server 2: FW VPN PPTP

User: admin Password: ••••••

Path: /home/admin

☑ Enable server 3

FTP server 3: FW_CL_10.3.0.111-0

User: user Password: •••

Path: /home/user

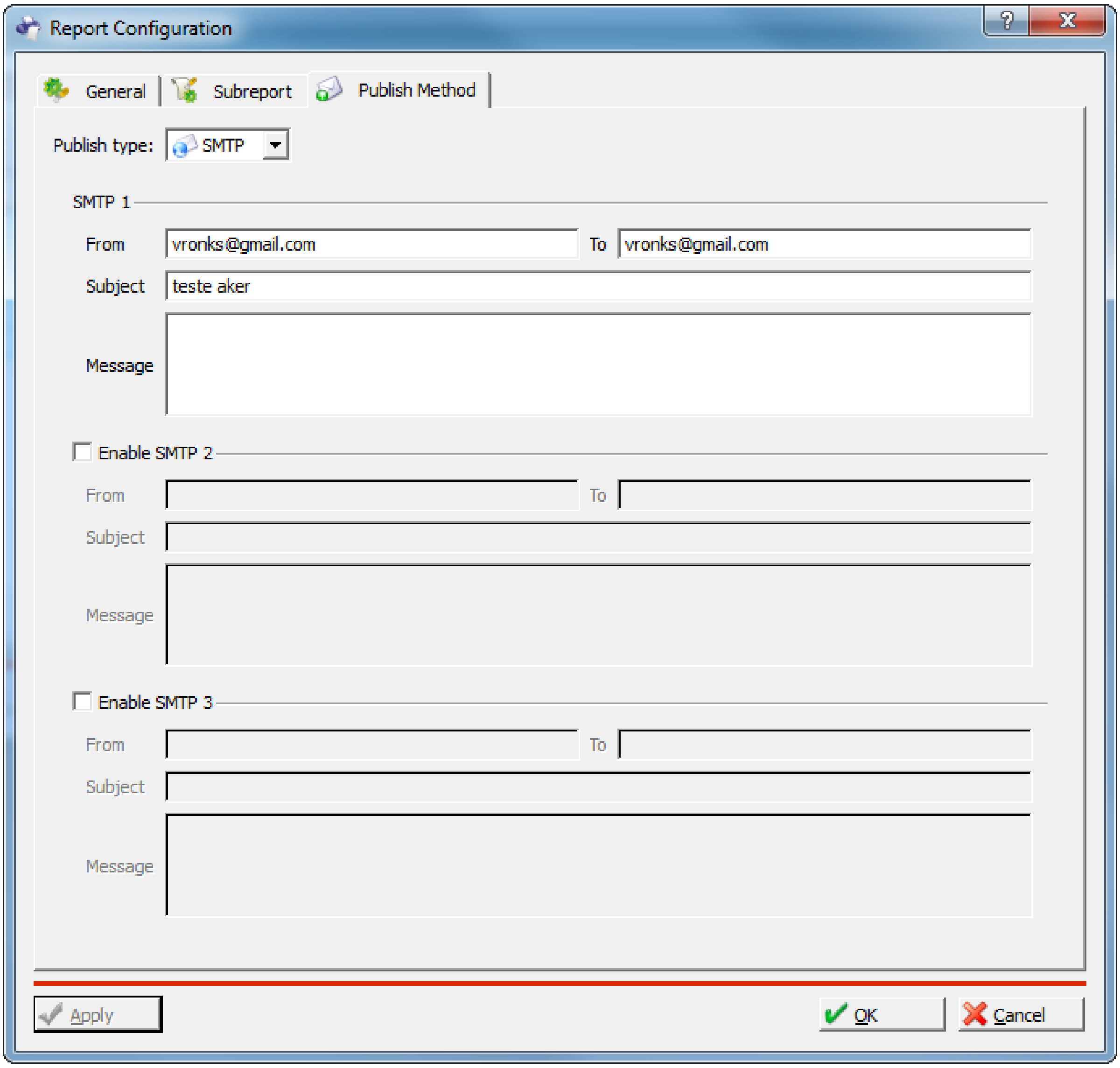
Image 355 – report configuration – Publish Method.

SMTP Method

In this tab you will be able to indicate up to three recipients, where the reports will be sent via e-mail.

How to use:

- Type the sender’s address (**"From"**);
- Type the recipient’s address (**"To"**);
- Type the **"Subject"**;
- If you wish a message can be included in the **“Message”** field.



Publish type: SMTP

SMTP 1

From vronks@gmail.com To vronks@gmail.com

Subject teste aker

Message

☐ Enable SMTP 2

From To

Subject

Message

☐ Enable SMTP 3

From To

Subject

Message

Image 356 –Report configuration –SMTP method.

Option Generate daily report now

This option allows the generation of reports in real-time (i.e. the firewall administrator can generate reports whenever he wants to). The product will continue working normally, and when the report is ready, save it in the desired directory, following a window showing the report will be displayed. The tab *Publish Method* is not available when you are using the option *Generate daily report now (real-time).*

19.3. List of available reports

Bellow follows the types of available reports that can be generated:

1. Amount of web access per authenticator users;
2. Amount of web access per authenticator groups;
3. Amount of web access per access profile;
4. Amount of web access per source IP address;
5. Amount of web access per destination IP address;
6. Amount of TCP and UDP access (each service) per authenticator groups;
7. Amount of access per web pages (domain), the selection of the most accessed pages is possible;
8. Amount of access per web pages (domain), the selection of the most accessed pages per authenticator groups is possible;
9. Amount of access, related the most accessed web pages and users;
10. Amount of blocked access per user, the selection of users with greater number of requests to forbidden pages is possible;
11. Amount of downloads made (HTTP and FTP), the selection of the most downloaded files is possible;
12. Traffic volume (kbps or Mbps) processed by the firewall, in periods of five minutes;
13. Website categories;
14. Downloads;
15. Blocked websites;
16. Blocked categories;
17. Blocked downloads;
18. Web IPs;
19. Blocked web IPs;
20. Destination IPs;
21. Blocked destination IPs;
22. IPs and services;
23. IPs and blocked services;
24. Services;
25. Blocked services;
26. Incoming traffic;
27. Outcoming traffic;
28. Recipient of delivered e-mails;
29. Recipient of rejected e-mail;
30. IP address of delivered e-mails;
31. IP address of rejected e-mails;
32. Recipient domain of delivered e-mails;
33. Recipient domain of blocked e-mails;
34. Quota – consumption of bytes;
35. Quota – consumption of time;
36. MSN – duration of chat;
37. MSN – chat log;
38. Web traffic accounting – consumed upload;
39. Web traffic accounting – consumed download;
40. Web traffic accounting– consumed time;

41. Traffic accounting of downloads – consumed upload;
42. Traffic accounting of downloads – consumed download;
43. Traffic accounting of downloads – consumed time;
44. FTP traffic accounting- consumed upload;
45. FTP traffic accounting- consumed download;
46. User who have accessed a website;
47. Users who have been blocked attempting to access a website.

Logs and events scheduled exports

20. Logs and events scheduled exports

This chapter shows how to configure the logs and events scheduled exports.

The records of logs and events are exported in the TXT or FTP format, and they are published via PFT in up to 3 different websites or locally in a firewall folder.

20.1. Accessing the logs and events scheduled exports

To gain access to the *logs and events scheduled exports* window follow the steps bellow:

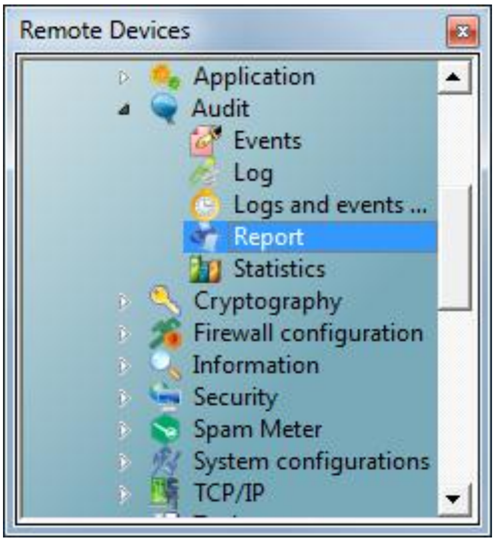

Remote Devices
Application
Audit
Events
Log
Logs and events ...
Report
Statistics
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 357 – Access window (*logs and events scheduled exports)*.

- Click on the *Audit* menu;
- Select *logs and events scheduled exports*.

20.2. Configuring the *logs and events scheduled exports*

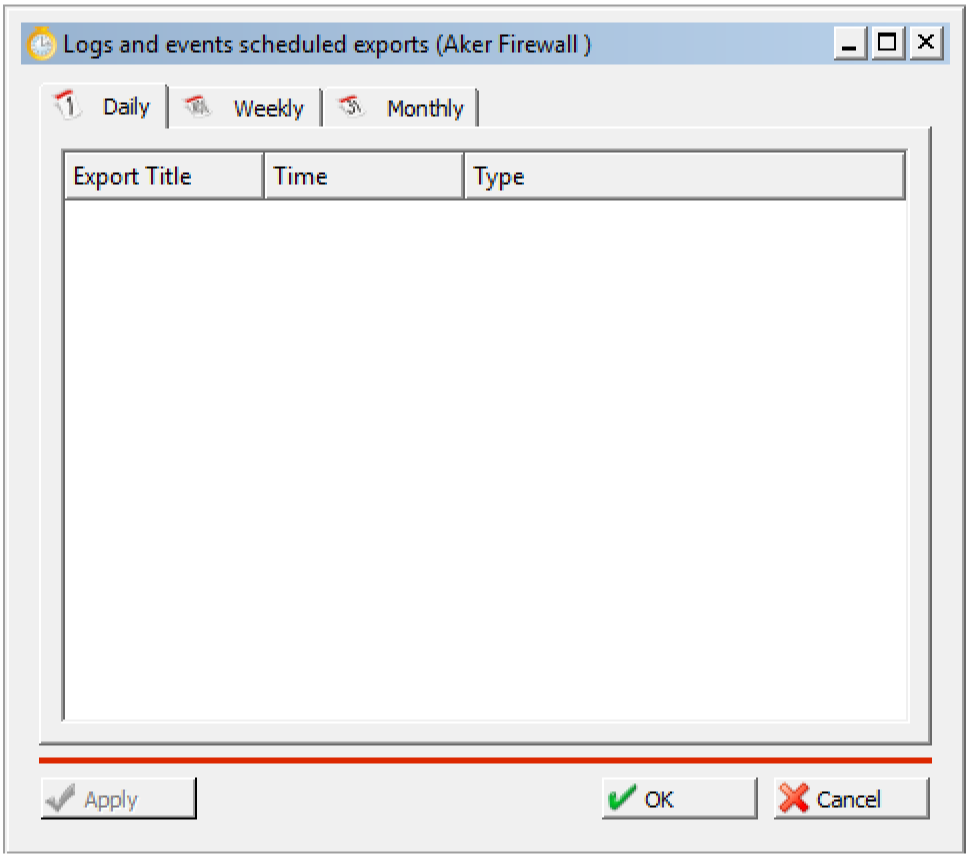

Logs and events scheduled exports (Aker Firewall)
Daily
Weekly
Monthly
Export Title
Time
Type
Apply
OK
Cancel

Image 358 – Logs and events scheduled exports – Daily.

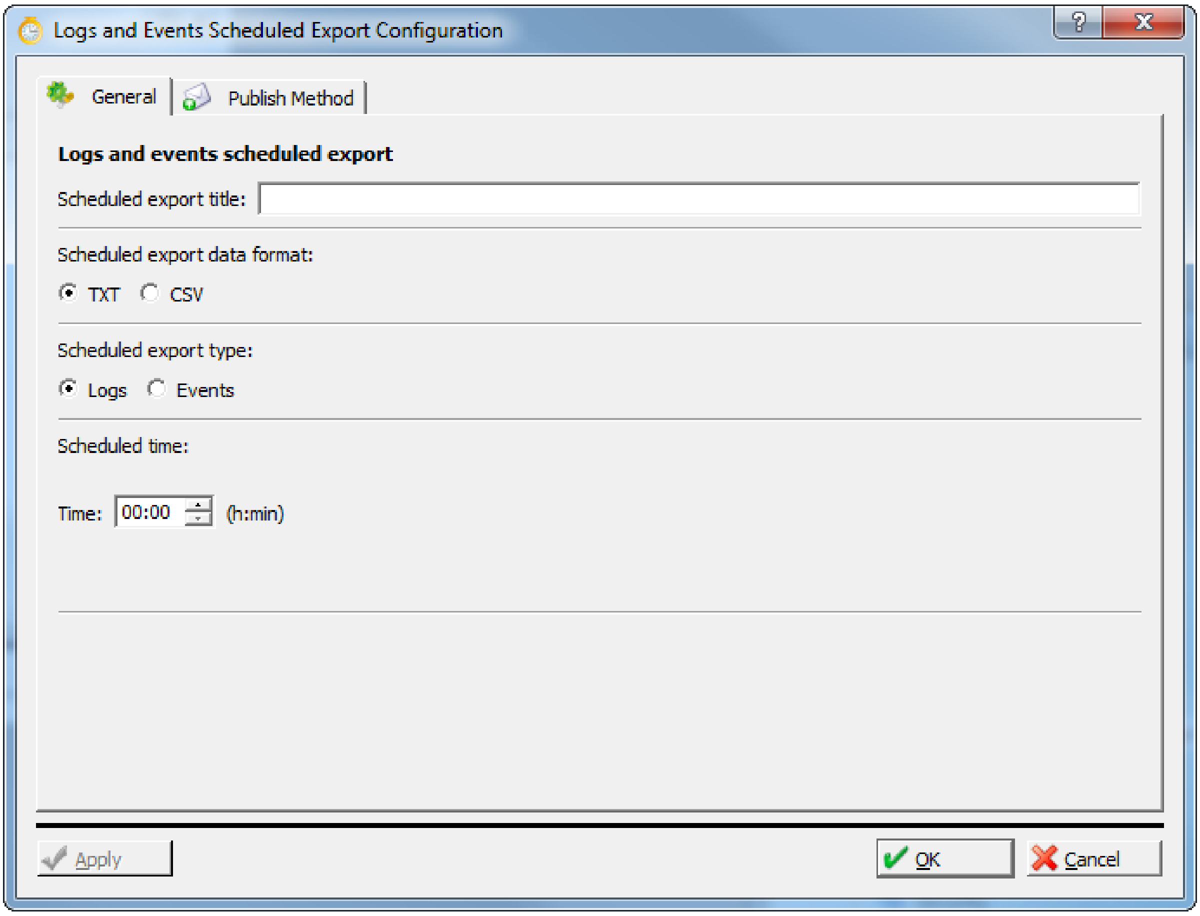
This window is composed by three types of schedules: "Daily", "Weekly" and "Monthly".

In order to run any export, you have to right-click on the report or double click on it. Then the window bellow will be displayed. In case no report is selected you will have only the option *Insert.*

- **Insert:** This option includes a new repor.t

When attempting to add a new report two tabs will be presented, the description of them follows bellow:

General Tab


Logs and Events Scheduled Export Configuration
General
Publish Method
Apply
OK
Cancel

Logs and events scheduled export

Scheduled export title:

Scheduled export data format:
● TXT ○ CSV

Scheduled export type:
● Logs ○ Events

Scheduled time:

Time: 00:00 (h:min)

Image 359 – Logs and events scheduled export configuration- general tab.

- **Scheduled export title:** Assign a name to the export.
- **Scheduled export data format**: Defines the format that the report will be generated. The format options are:
  - TXT;
  - CSV.

- **Scheduled export type:** Defines which information will be exported:
  - Logs;
  - Events.
- **Scheduled time:** Defines the time that the export will be performed.

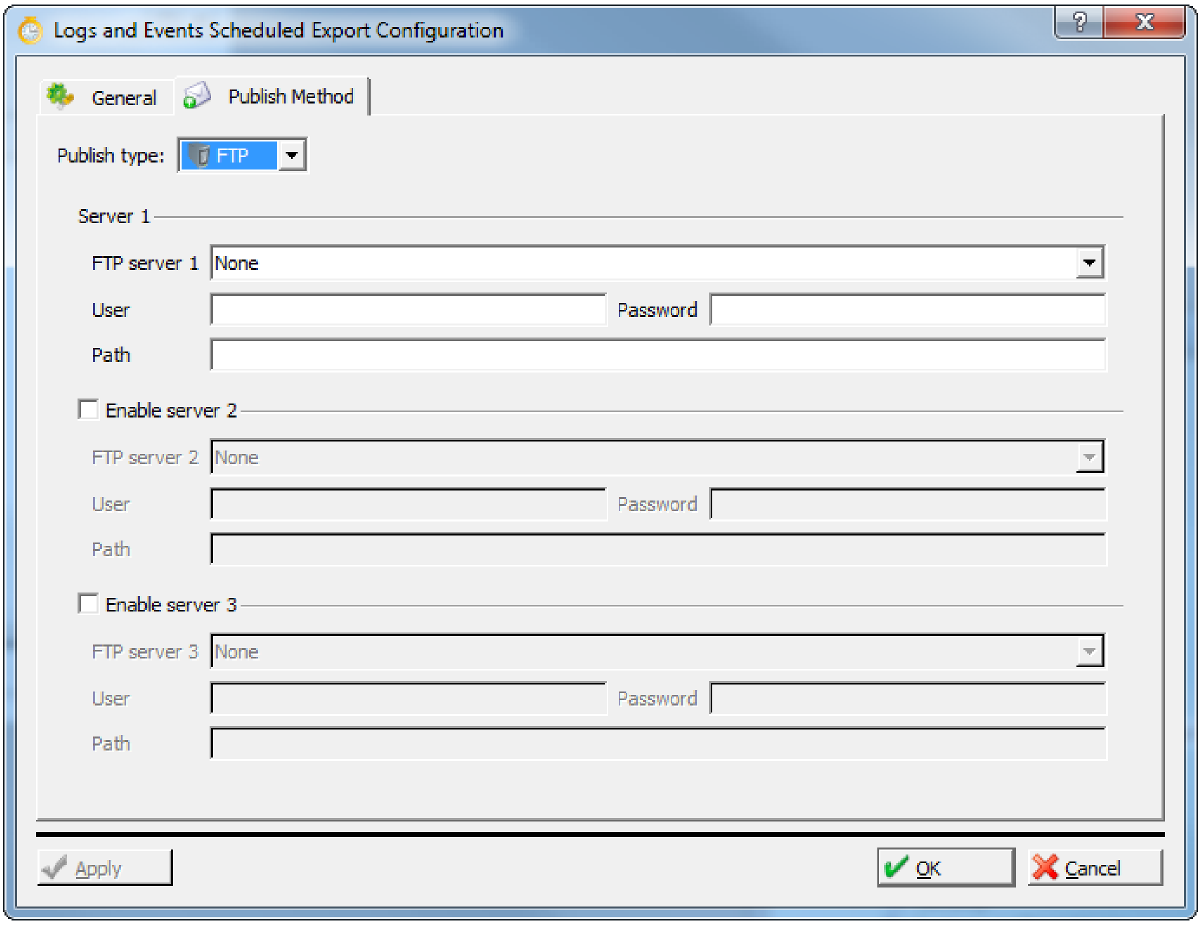
Publish Method

FTP:

In this tab, the user can indicate up to three servers where the data will be sent via FTP.

How to use:

- Select the server or servers;
- Type the user;
- Type the password;
- Type the path of the report destination;


Logs and Events Scheduled Export Configuration
General
Publish Method
Apply
OK
Cancel

Publish type: FTP

Server 1
FTP server 1 None
User
Password
Path

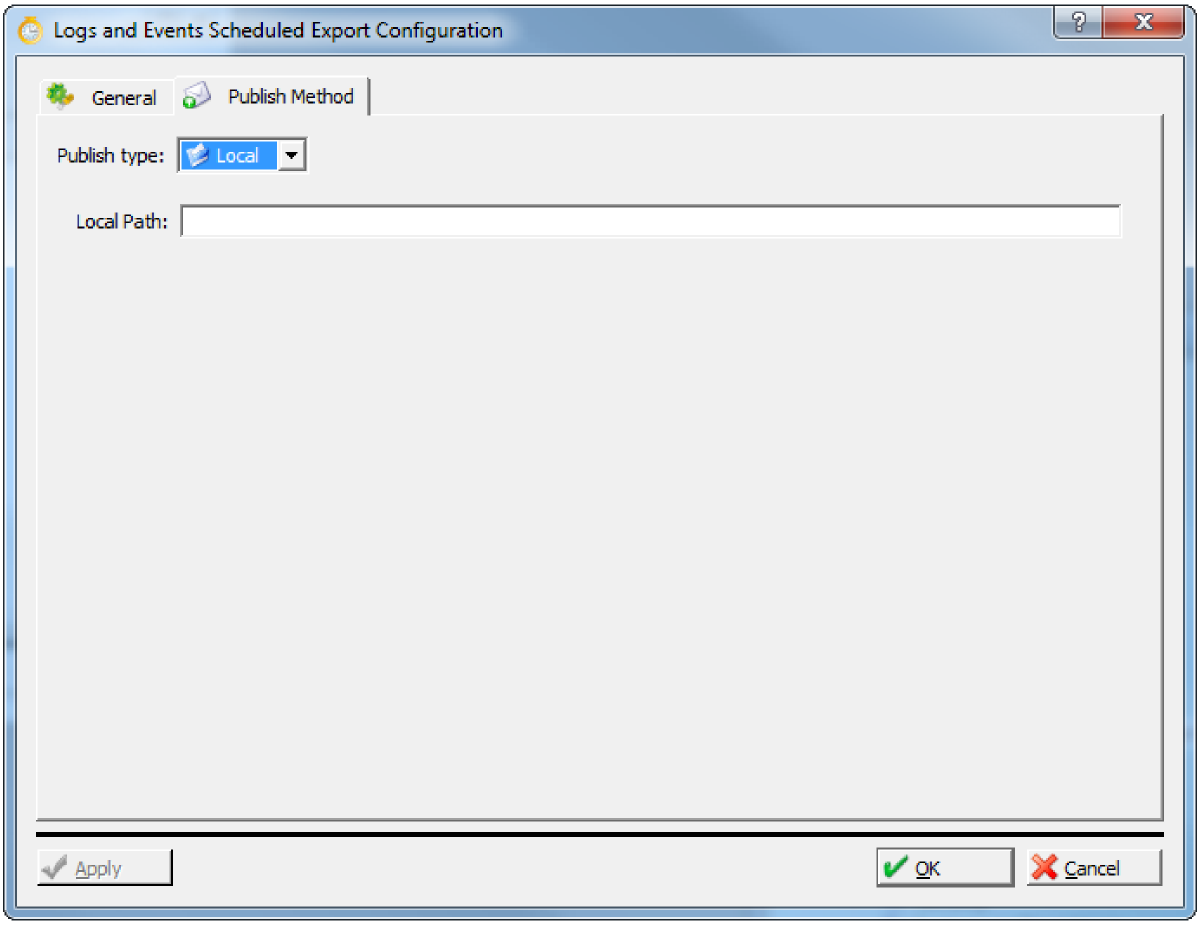
☐ Enable server 2
FTP server 2 None
User
Password
Path

☐ Enable server 3
FTP server 3 None
User
Password
Path

Image 360 – Logs and events scheduled export configuration – Publish Method.

Local:

In this tab, user will be able to indicate which local path of Aker Firewall the exported data will be saved.


Logs and Events Scheduled Export Configuration
General
Publish Method
Apply
OK
Cancel

Publish type: Local

Local Path:

Image 361 – Logs and events scheduled export configuration – Publish type.

Working with proxies

21. Working with proxies

This chapter will show all the information required to understand the operation of Aker Firewall proxies. Specific details of each proxy will be discussed in the next chapters.

21.1. Planning the installation

What are proxies?

Proxies are specialized programs that usually run in firewalls and are used as a bridge between the Intranet of an organization and the external servers. Its operation is simple: they wait for a request of Intranet, then pass this request to the remote server in the external network, and send the answer back to the internal client.

Most of the time the proxies are used by all the clients of one subnet and, due to its strategic point, they normally implement a cache system for some services. Moreover, as the proxies work with application data, a different proxy for each service is necessary.

Traditional proxies

In order to make a host use the services of a proxy, the host must know that the proxy exists, i.e. the host has to know that instead of connecting to the remote server, it should connect to the proxy and pass its requests to it.

There are some clients that already have their own proxy support (most of the existent browsers can be mentioned as examples of this type of client). To use the proxy functions, in this case, it is only necessary to configure them to do it. Most of the clients, however, are not ready to work this way. If this is the case, the only possible solution is to change the TCP/IP stack in all the client hosts, in order to make that all connections be transparently passed to the proxies.

This approach brings several difficulties, apart from being extremely hard to modify all the client hosts, most of the time there is no way to modify the TCP/IP implementation of some platforms, making the clients of these platforms unable to use the proxy.

Another problem of the traditional proxies is that they can only be used for access from internal to external hosts (it is not possible to require external clients to pass their requests o your proxy in order to the proxy pass them to the internal server).

The Image bellow illustrates the basic operation of a traditional proxy:

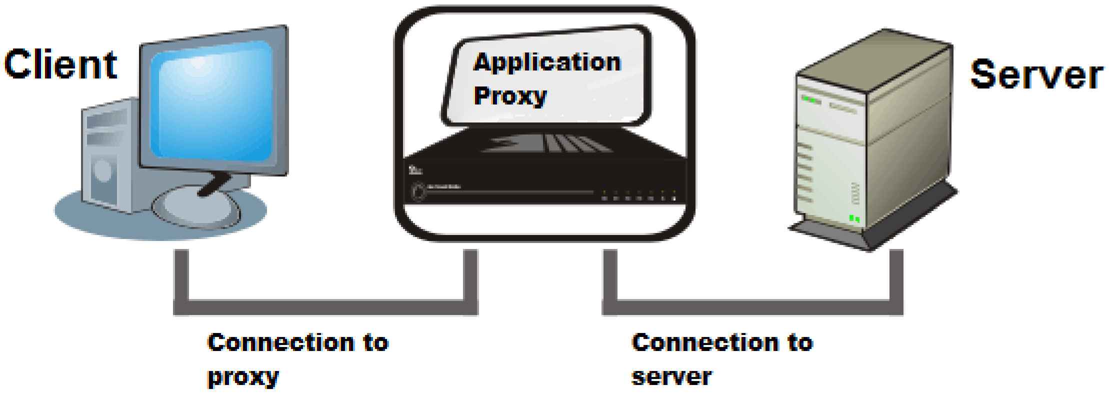


Image 362 – Basic operation of a traditional proxy.

Transparent proxies

Aker Firewall introduces a new concept of firewall, with the use of transparent proxies. These transparent proxies are capable of being used without any modification on the clients and servers, because none of them will know about their existence.

Its operation is very simple: whenever the firewall decides that a specific connection must be treated by a transparent proxy, this connection is redirected to the appropriate proxy. When the connection is received, the proxy opens a new connection to the remote server and passes the requests of the client to this server.

The great advantage of working like this is the possibility to offer an additional security for specific services without losing the flexibility and without modifying any of the clients or servers. Besides, it is possible to use transparent proxies in internal or external requests, indifferently.

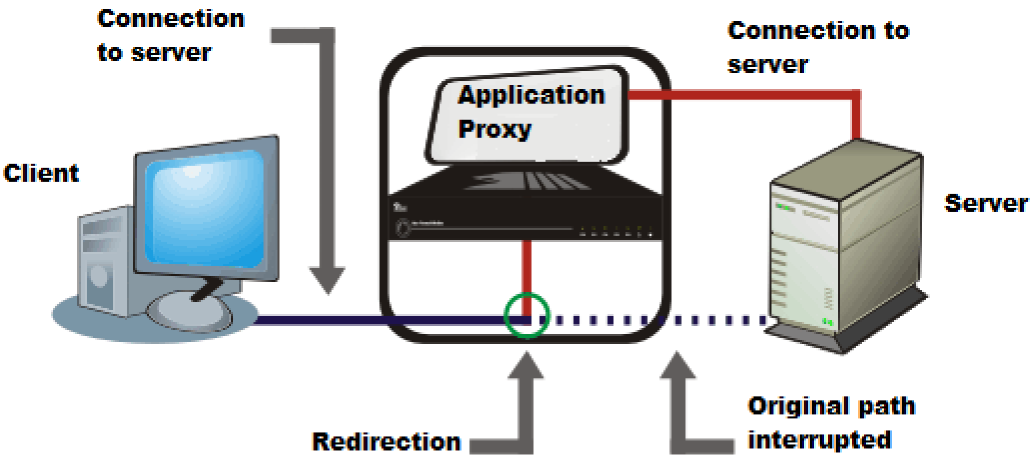

Connection to server
Connection to server
Application Proxy
Client
Server
Redirection
Original path interrupted

Image 363 – Basic operation of a transparent proxy

Transparent proxy and content

Aker Firewall introduces a new development related to the transparent proxies: the contents. To understand them, let us first analyze a network topology, where its existence is necessary:

Suppose there is an Aker Firewall connected to three distinct networks, called ***A***, ***B*** and ***C*,** and that the networks ***A*** and ***B*** are networks from two departments of the same company and network ***C*** is the Internet. Suppose there is a SMTP server shared by networks ***A*** and ***B*** to send and receive e-mails. All this is showed in the drawing bellow:

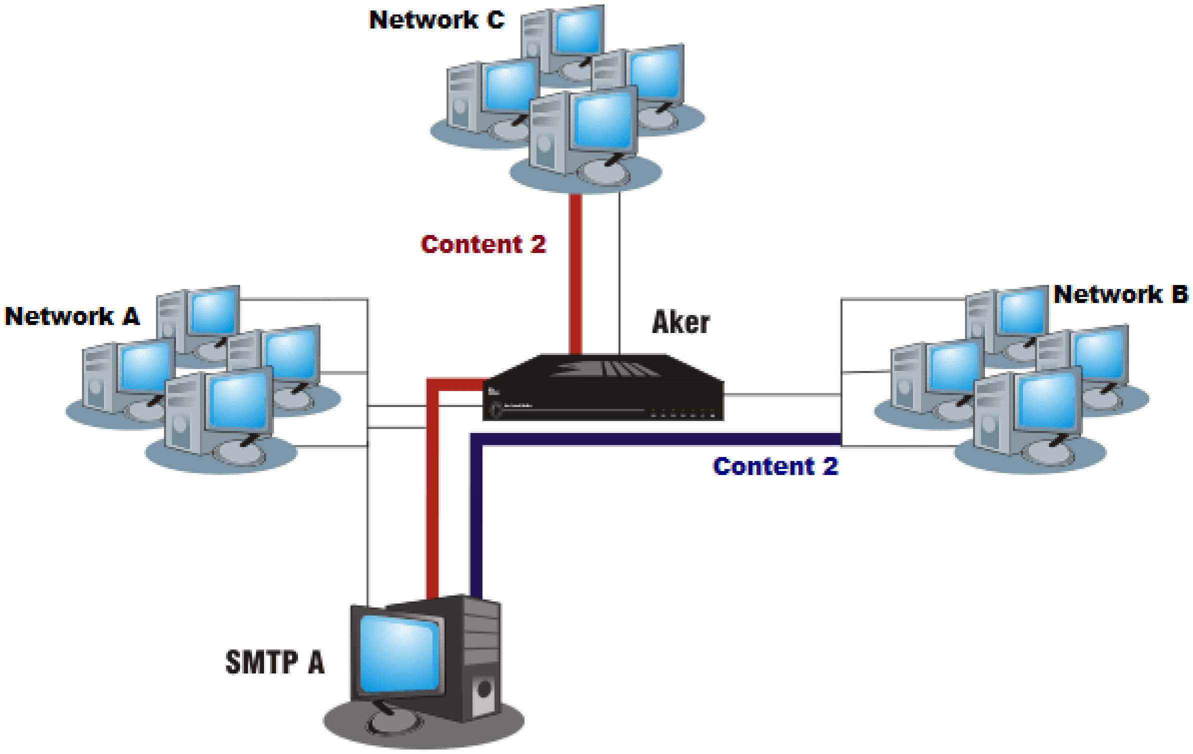


Image 364 – Transparent proxies and content.

Now, suppose you want to configure the firewall to redirect all the SMTP connections to the SMTP proxy, in order to provide better protection and more control over this traffic.

It is important to have a way to treat distinctly the connections for **A** with ***B*** and ***C*** as sources: The network ***B*** will use the SMTP server of **A** as a relay when sending its e-mails, however the same will not be allowed from the network **C**. You may want to limit the maximum size of the messages originated in the network **C**, to avoid attacks of denial of service based on lack of disc space, without, at the same time, limiting the size of the messages originated in the ***B*** network.

To make this differential treatment possible, the *contents* concept was created. *Contents* are nothing more than different configurations for the transparent proxies in order to enable different operation modes for different connections.

In the last example, two contents could be created: one to be used in the connection from ***B*** to ***A*** and the other from ***C*** to ***A***.

Aker Firewall proxies

Aker Firewall implements transparent proxies for FTP, Telnet, SMTP, POP3 and HTTP protocols and non-transparent proxies for the services accessed through a WWW (WORLD WIDE WEB) browser (FTP, Gopher, HTTP and HTTPS) and for clients that support the SOCKS protocol. To use the non-transparent proxies, a client that can be configured such as the proxy is needed. Among the clients that support this type of configuration are the Netscape Navigator(TM) and the Internet Explorer(TM).

The transparent proxies can be used to control external access to the Intranets as well as access from the Intranet to external services. Non-transparent proxies can only be used by a host in the Intranet.

Aker Firewall also allows the implementation of proxies created by users, which are proxies created by third-parties using the proxy development API that Aker Security Solutions provides. The objective is to allow that institutions that have specific protocols be capable of develop support in the firewall for these protocols.

Aker Firewall authenticators

Aker Firewall SOCKS, Telnet and WWW (WORLD WIDE WEB) proxies support user authentication, i.e. they can be configured to allow a specific session be established only if the user identifies himself through a name and a password for the firewall, and then this user will be allowed to start the desired session.

The main problem with this kind of authentication is how the firewall will validate the received names and passwords. Some products require all users to be registered in a firewall database or be valid users of the host that the firewall is running on. Both methods have a great limitation because they do not use the user's database usually present in a local network.

In Aker Firewall, a more versatile and simpler solution has been chosen: instead of demanding the users to be registered in the firewall, they are validated in their own local network servers, either Unix or Windows NT.

For the firewall know in which servers it must authenticate the users, and also to allow secure communication with these hosts, the concept of *authenticators* was created. Authenticators are Unix or Windows NT hosts that run a program called *Authentication Agent.* This program is distributed as part of Aker Firewall and its basic function is; serve as interface between the firewall and the remote databases.

In order to make Aker Firewall use a database in a remote server, you need to follow the steps bellow:

1. Install and configure the authentication agent in the host where the users database resides (this procedure will be described in the sections ***Installing the authentication agent*** in Unix and ***Installing authentication agent in Windows NT***).
2. Register an entity of the authenticator type with the address of the host where the agent was installed and with the correct access password (for further information on how to register an entity, refer to the chapter **Registering Entities**).

3. Indicate to the firewall that it must use the authenticator registered in the step 2, to perform the user’s authentication (this procedure will be described in the chapter **Configuring the authentication parameters**).

Aker Firewall 6.5 is incompatible with authenticators of versions older than 4.0. In case an upgrade of an old version has been done and the firewall is performing user authentication, it is necessary to reinstall the authenticators.

It is also possible to perform authentication through LDAP and RADIUS protocols. In this case, there is no need to install the authenticators on the server hosts, being it enough to create the authenticators of the corresponding types and indicate to the firewall that the authenticators need to be used, according to steps 2 and 3 listed above.

21.2. Installing the authentication agent on Unix Platforms

To install the authentication agent is necessary download the **Authentication Agent** specific for you system at Aker’s website (http://www.aker.com.br), after downloading unzip the file and execute the following command:

```
#/ ./aginst
```

The symbol # represents the shell prompt while you are logged as root. Do not type it as part of the command.

The installation program will copy the agent executable file (*fwagaut*) to the/usr/local/bin directory and a configuration file model (*fwagaut.cfg*) to the /etc directory. After the installation is complete, it is necessary to customize this file, as described on the next section.

If you have answered *"Yes"* when the installation program asked if you wanted to start the agent automatically on each boot, an entry will be created on an initialization file in order to start the agent automatically. The name of this initialization file depends on the Unix version that has been used.

Syntax of the configuration files of the authentication agent

After installing the authentication agent, it is necessary to create a configuration file with the firewalls’ addresses that can use it and the access passwords of each one. This file is in text format and can be created by any editor.

The configuration file of the authentication agent must have its access rights configured in a way that only the root user can read or change its contents. To do it, the command *chmod* can be used, with the following syntax: #chmod 600 *file_name*

Its syntax is:

- Each line must have the IP address of an Aker Firewall that will use the agent, one or more blank spaces or *tab* characters, and the access password that the firewall will use in the communication.
- Lines beginning with the character #, as well as blank lines, are ignored

An example of a possible configuration file is displayed below:

```
# Configuration files for Aker Firewall 6.5 authentication agent
#
# Syntax: Firewall IP address and access password (in each line)
```

```
#
# The password must not have spaces and the password goes up to 31 characters
#
# Lines beginning with the '#' are considered comments
# Blank lines are allowed

10.0.0.1 password_test
10.2.2.2 123password321
```

The default place for the agent configuration file is **/etc/fwagaut.cfg**, however it is possible to create it with any other name or in another directory, since it is informed to the agent at startup. This will be displayed in the next section.

Authentication agent execution syntax

The authentication agent for Unix has the following execution syntax:

```
   fwagaut [-?] [-c FILE_NAME] [-s <0-7>] [-q]
   Where:
-? shows this message and returns to the shell prompt
-c Specifies the name of an alternate configuration file
-s Specifies the syslog facility where the authenticator
   messages will be sent to. 0 = local0, 1 = local1, ...
-r Allows root user validation
-e Accepts users with empty passwords
-q Quiet mode. Do not show any messages upon startup
```

Suppose that the agent is located in the /usr/local/bin directory and the configuration file has been created with the name/usr/local/etc/fwagaut.cfg. In this case, to start the agent, the command line would be:

```
/usr/local/bin/fwagaut -c /usr/local/etc/fwagaut.cfg
```

In case you want to start the agent with the configuration file on the default location, it is not necessary to use the option **-c**, just run it with the command:

```
/usr/local/bin/fwagaut
```

The authentication agent must be started by the root user.

When any modification is made on the configuration file, it is necessary to inform the agent about this modification, if the agent is running. To do it, the following command must be run:

```
#kill -1 pid
```

"*pid*" is the process number of the authentication agent. To get this number, execute the command:

#ps -ax | grep fwagaut can be used in hosts based on Unix BSD,

Or

#ps -ef | grep fwagaut in hosts based on Unix System.

The authentication agent listens to requests on port 1021/TCP. There cannot be any other application using this port while the agent is active.

21.3. Installing the authentication agent on Windows Server^{tm}

The installation of authentication agent for Windows Server^{tm} is very simple. Download the Authentication Agent for you system at Aker's website (http://www.aker.com.br).

The program will first display a window asking for confirmation to proceed with the installation. To continue the installation, is necessary to answer "**Yes**" to the question. Following a window with the license will be displayed and then the window where the installation directory can be specified.

After selecting the installation directory, it is necessary to click on the **Copy files** button, which will perform the agent installation. This installation consists in the creation of a directory with the agent files, called **fwntaa**, in the **Program Files** directory, in the creation of a group called *Aker Firewall* with the configuration and agent removal options, and the creation of a service called **Aker Firewall Authentication Agent**. This is a normal service of the Windows Server^{tm} and it can be stopped or started through the *Control Panel*, in the *services* icon.

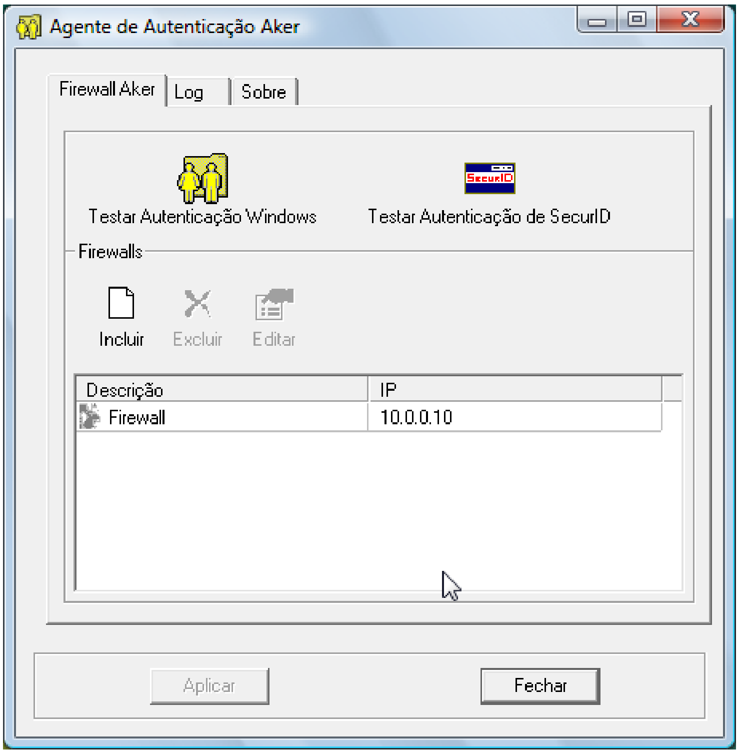
The authentication agent listens to requests on ports 1016/TCP and 1021/TCP. There cannot be any other application using this port while the agent is active.

21.4. Configuring authentication agent for Windows Server^{tm}

After the installation of the agent, it is necessary to proceed with its configuration. This configuration allows the registration of all the firewalls that will use the agent, as well as the definition of the messages that will be produced by the agent while it is running. Differently from the authentication agent used for Unix, this configuration is done through a different program.

To gain access to the configuration program, it is necessary to click on the *Start* menu, select the *Aker Firewall group* and inside this group, then click on the option *Configure authentication agent*. After the previous steps are done, the agent configuration window (which consists of 3 tabs) will be displayed.

Aker authenticator agent – Firewall configuration


Agente de Autenticação Aker
Firewall Aker
Log
Sobre
Testar Autenticação Windows
Testar Autenticação de SecurID
Firewalls
Incluir
Excluir
Editar
Aplicar
Fechar

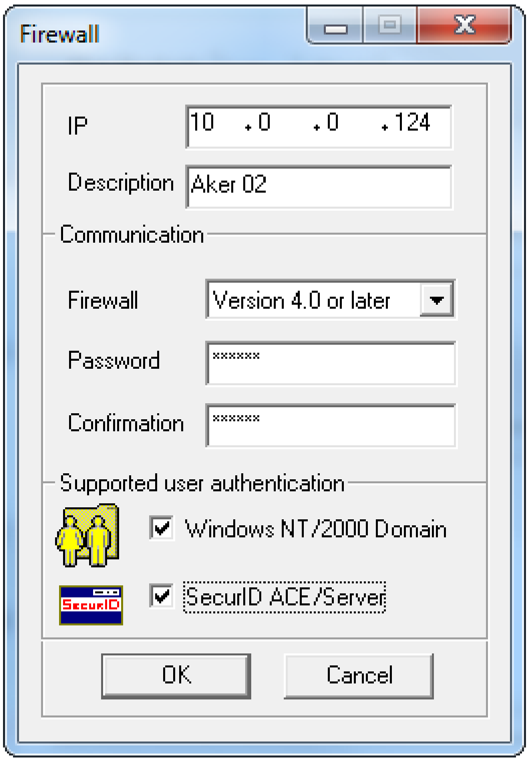
Descrição	IP
Firewall	10.0.0.10

Image 365 – Authentication Agent (Aker)

This tab contains all the configuration options of the agent. In the upper part of the window there are two buttons that allow the administrator to test the authentication of a user, in order to check if the agent is working correctly. In the lower part of the tab there is a list of all firewalls authorized to connect to the authentication agent.

In order to add a new firewall to the list, just click on the **“Add”** button, located in the toolbar. To remove or edit a firewall, just select the firewall to be removed or edited and click on the corresponding option in the toolbar.

For the ***Add*** or ***Edit*** options, the following window will be displayed:



IP: 10 . 0 . 0 . 124
Description: Aker 02
Firewall: Version 4.0 or later
Password: ******
Confirmation: ******
☑ Windows NT/2000 Domain
☑ SecurID ACE/Server

Image 366 – Authentication Agent

IP: It is the IP address of the firewall that will connect to the agent.

Description: It is a field, used only for documentation purposes.

Password: It is the password used to generate the authentication and encryption keys, used on the communication with the firewall. This password must be the same as the one configured in the entity. For further information, refer to the chapter **Registering Entities**.

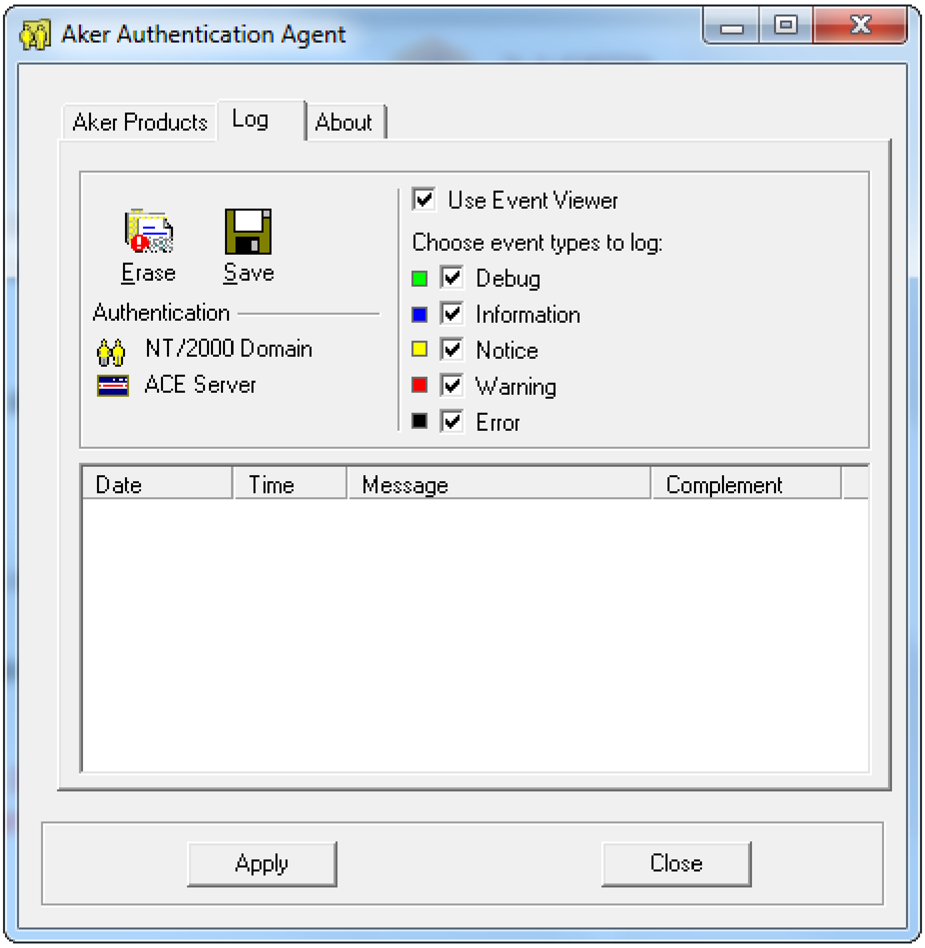
Confirmation: This field is used only to check if the password was typed correctly. It must be typed exactly as the *Password* field.

User authentication methods: This field indicates which user authentication methods will be accepted. It consists of two options which can be selected independently:

Windows NT/2000 domain: If this option is checked the agent will perform user authentication using the user database from Windows NT/2000.

SecurID ACE/Server: If this option is checked the agent will perform user authentication consulting the SecurID ACE/Server.

Log tab


Aker Authentication Agent
Aker Products
Log
About
Erase
Save
Authentication
NT/2000 Domain
ACE Server
Date
Time
Message
Complement
Apply
Close

☑ Use Event Viewer

Choose event types to log:

🟩 ☑ Debug
🟦 ☑ Information
🟨 ☑ Notice
🟥 ☑ Warning
⬛ ☑ Error

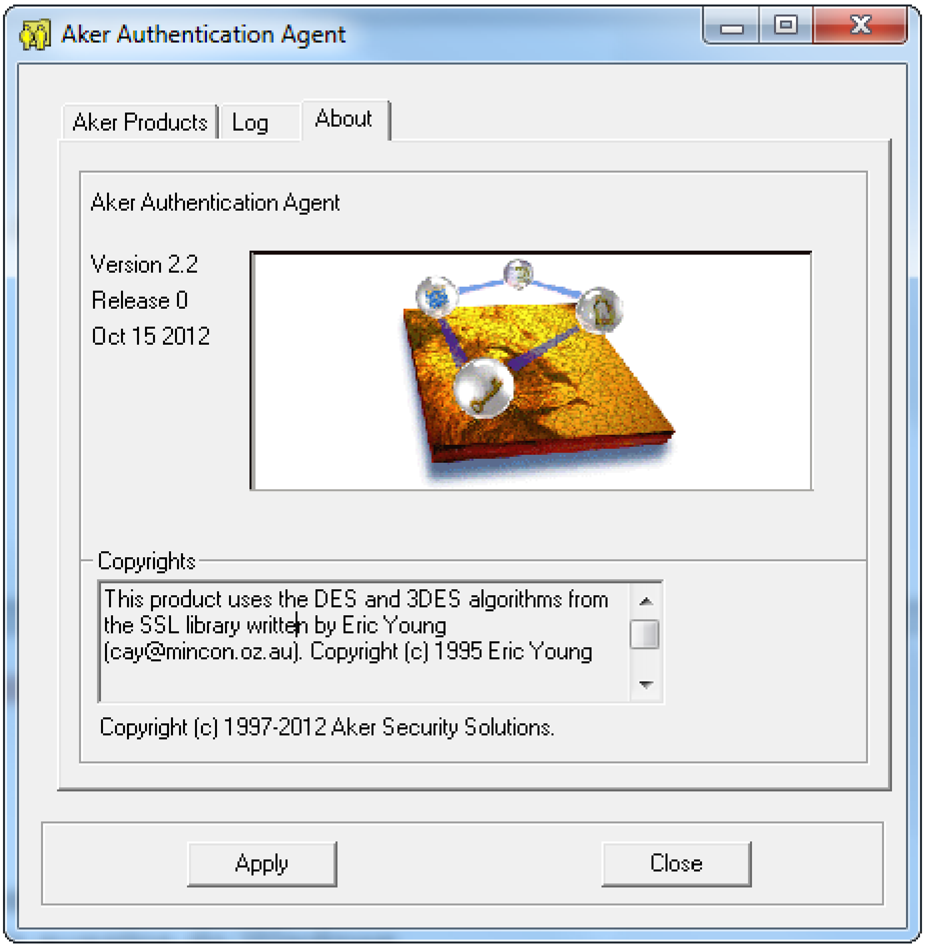
Image 367 – Authentication agent – Log.

This tab is really useful to monitor the authentication agent operation. It consists of a list with several messages, sort by time. Besides each message, there is a colored icon representing its priority. The colors have the following meaning:

Blue	Debug
Verde	Information
Yellow	Notice
Red	Warning
Black	Error

In case you do not want specify a priority of messages, just uncheck the check-box on its left.

The option **Use event viewer**, if this option is checked, it sends all messages to Windows event viewer.



Aker Authentication Agent

Version 2.2
Release 0
Oct 15 2012

This product uses the DES and 3DES algorithms from the SSL library written by Eric Young (cay@mincon.oz.au). Copyright (c) 1995 Eric Young

Copyright (c) 1997-2012 Aker Security Solutions.

Image 368 –Authentication agent (About)

This is an informative tab and is useful to get some pieces of information about the client, such as its version and release.

Removal of the authentication agent for NT

To make the removal of an authentication agent for NT easier, there is a utility that does it automatically. To start it click on the *Start* menu, select the *Aker Firewall* group and in this group select the option *Remove authentication agent*. After this, a window asking for confirmation will be displayed.

To uninstall the agent, click on the **Yes** button. To cancel the removal, click on the **No** button**.**

Configuring authentication parameters

22. Configuring the authentication parameters

This chapter shows which are and how the authentication parameters must to be configured, these parameters are essential to make possible the user authentication through the firewall.

What are authentication parameters?

Authentication parameters are used to inform the firewall which authentication methods are allowed, which authenticators must be searched to authenticate a specific user, and in which order. In addition, they control the way the search is performed, allowing for authentication flexibility

22.1. Using the remote Interface

To gain access to the authentication parameters, follow the steps bellow:

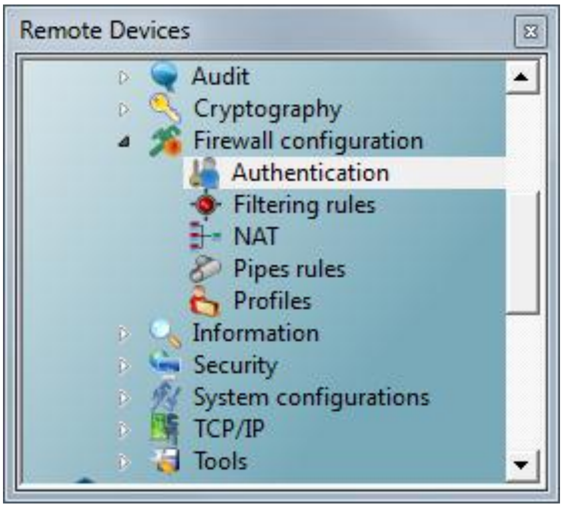

Remote Devices
Audit
Cryptography
Firewall configuration
Authentication
Filtering rules
NAT
Pipes rules
Profiles
Information
Security
System configurations
TCP/IP
Tools

Image 369 – Access window: Authentication.

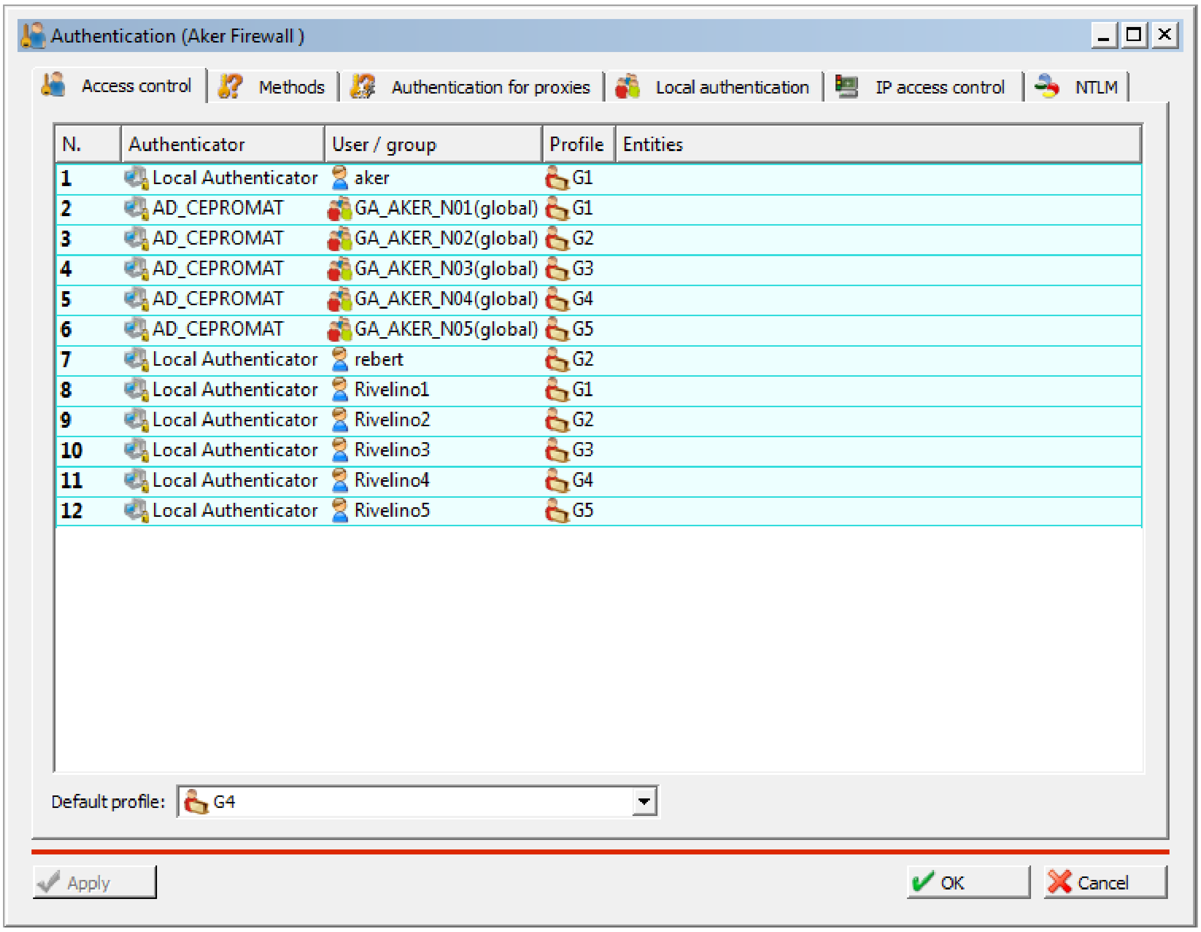
- Click on the *Firewall configuration* menu.
- Selection *Authentication.*

This window consists of six tabs: the first one is the ***Access Control tab***, where users and groups from authenticators are associated with access profiles. The configuration procedure is explained with more details in the chapter ***User Access Profiles***. In the second tab, the **Authentication Methods** are chosen. User/Password, Certification Authorities (PKI), and Token (SecurID) authentication parameters are defined here. The third tab configures the **Authentication for**

Proxies. In the fourth tab configures the **Local authentication** and in the fifth tab the **IP Access Control** is configured. The sixth and last tab **NTLM** configures the firewall integration to Microsoft Active Directory (AD) and use the automatically login (more details about this will be seen in the chapter **User Access Profiles).**

- The **OK** button closes the Parameters Configuration window and applies all changes.
- **Apply** saves all changes to the firewall and keeps the window open.
- The **Cancel** button closes the window and discards any modification

Access Control tab



N.	Authenticator	User / group	Profile	Entities
1	Local Authenticator	aker	G1	
2	AD_CEPROMAT	GA_AKER_N01(global)	G1	
3	AD_CEPROMAT	GA_AKER_N02(global)	G2	
4	AD_CEPROMAT	GA_AKER_N03(global)	G3	
5	AD_CEPROMAT	GA_AKER_N04(global)	G4	
6	AD_CEPROMAT	GA_AKER_N05(global)	G5	
7	Local Authenticator	rebert	G2	
8	Local Authenticator	Rivelino1	G1	
9	Local Authenticator	Rivelino2	G2	
10	Local Authenticator	Rivelino3	G3	
11	Local Authenticator	Rivelino4	G4	
12	Local Authenticator	Rivelino5	G5	

Default profile: G4

Image 370 – Access authentication: Access control.

The access control window allows the creation of the association of users/groups with an access profile.

At the bottom of the window above there is a field called **Default Profile**, in this field is possible select the profile that will be assigned to users who do not fit in any association rule.

The last column when filled specifies the hosts and networks where the association is valid. If user fits in the rule, but he is in an IP address that is not in the registered hosts or network.

To assign a use or group with a specific access profile, follow the step below:

1. Right-click on the list of rules and select the option **Insert**;
2. Select the authenticator you wish to get the list of users or group, by right-clicking on the **Authenticator** field,;
3. Right-click on the *User/Group* field and select between the user or group list, then your list will be mounted automatically through the selected authenticator. In this list select the desired user or group.

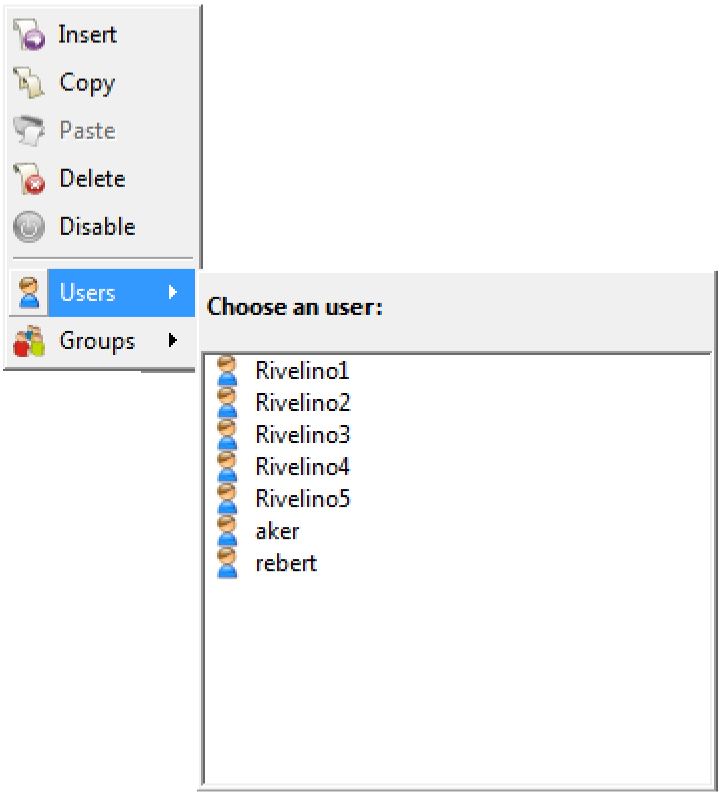

Insert
Copy
Paste
Delete
Disable
Users
Groups
Choose an user:
Rivelino1
Rivelino2
Rivelino3
Rivelino4
Rivelino5
aker
rebert

Image 371 – Access authentication: List of user or group.

4. Right-click on the *Profile field* to select the desired profile as the example below:

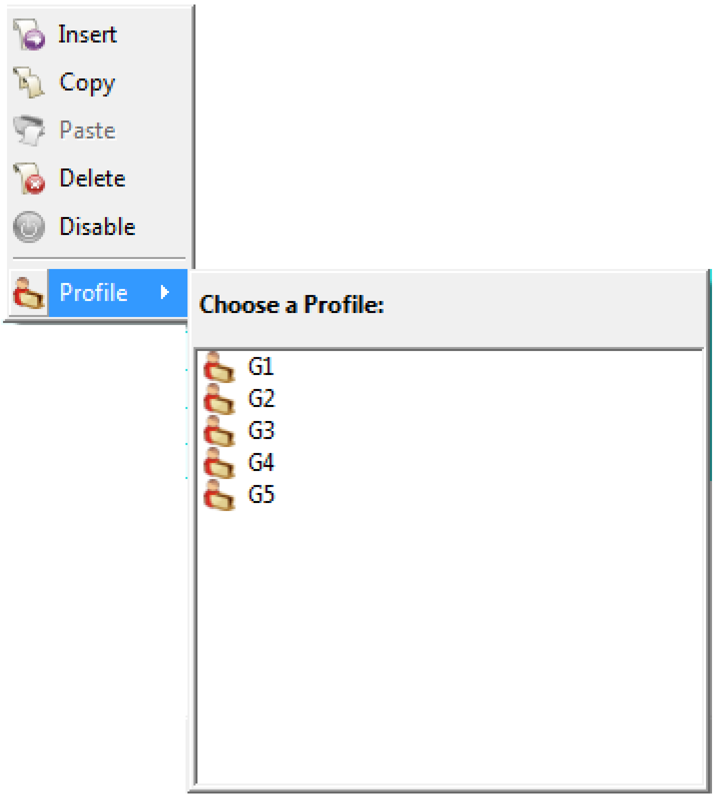


Image 372 – Access authentication: Choosing a profile.

5. If you want, you can drag few hosts, set or network entities to the entities field.

To remove a rule between user/group and a profile follow the steps bellow:

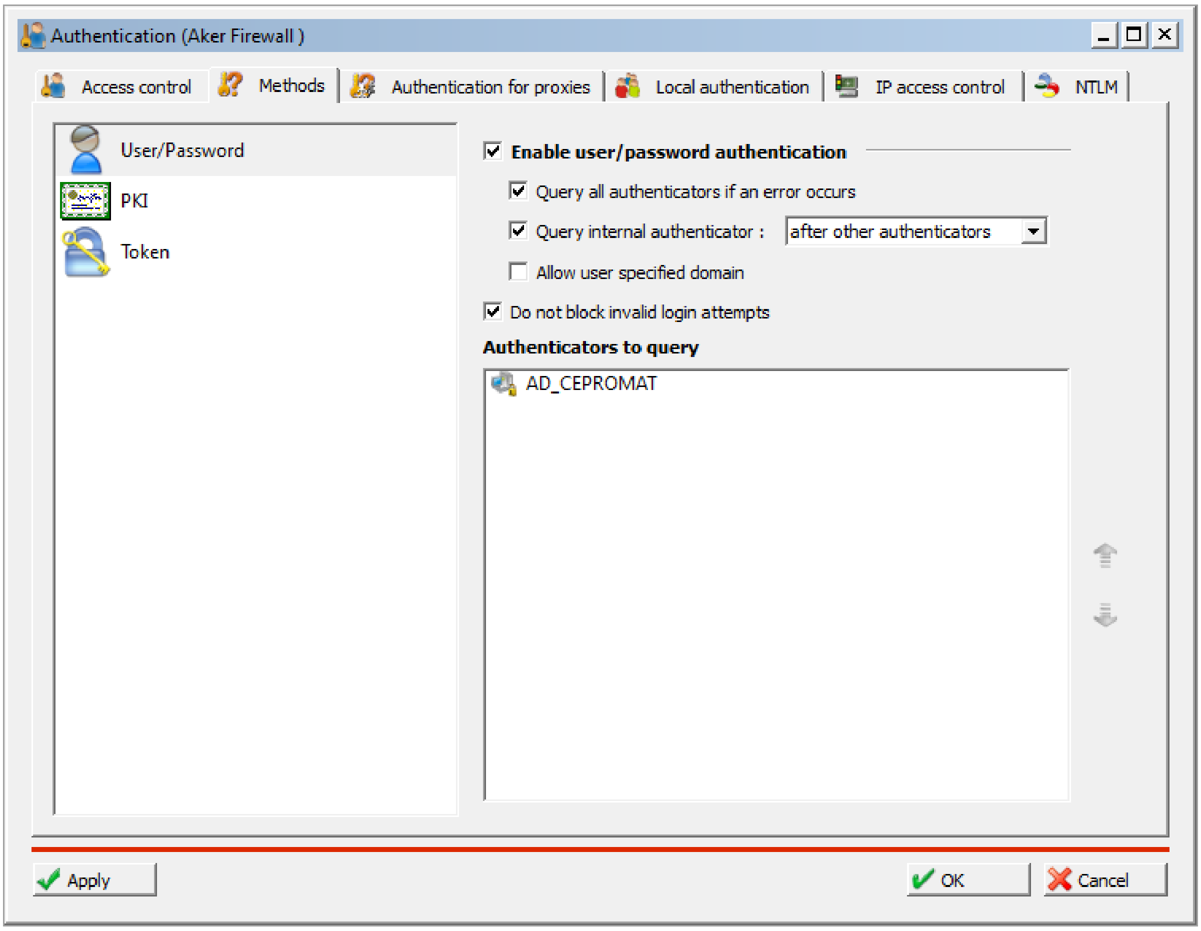
1. Select the rule you wish to remove
2. Click on **delete**.

To change a rule position in the list, follow the steps bellow:

1. Select the position you wish to move;
2. Drag it to the desired position.

The order of the association in the list is very important. When a user authenticate himself, Aker Firewall start a seach in the list looking for this user name or group that he belongs to. When the user is found the profile assigned to him will be used.

Methods tab



Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
User/Password
PKI
Token
Apply
OK
Cancel

☑ Enable user/password authentication

☑ Query all authenticators if an error occurs

☑ Query internal authenticator : after other authenticators

☐ Allow user specified domain

☑ Do not block invalid login attempts

Authenticators to query

AD_CEPROMAT

Image 373 – Access authentication: Methods.

Enable User/Password authentication: This option indicates if the firewall will accept or not, the users' authentication through name/password. If active, all other corresponding parameters must be configured.

Query all authenticators: This parameter indicates if the firewall should try to validate the same user with other authenticators on the list, whenever an authenticator returns an invalid password message.

If this option is checked, the firewall goes through all authenticators on the list, until it either receives a correct authentication response, or it reaches the end of the list. If this option is not checked, the search will terminate with the first authenticator that send response, being it a message of correct authentication, or a message of invalid password.

This option is only used for invalid password responses. If an authenticator responds that the user is not registered in its database, the firewall continues searching with the next authenticator on the list, regardless this option's value

Query internal authenticator: This parameter indicates if the firewall local user base (define in the local authentication tab) must to be queried to validate the users' password. If yes, you also need to choose between one of the option in the box next to the ***Query Internal authenticator*** if this base will be queried before or after other authenticators.

Allow user-specified domain: This parameter indicates if the user when authenticating can inform to the firewall which authenticator he wants to be validated at.

If this option is checked, users can add to their name a ***/*** (***slash)*** and an authenticator name. This will make the authentication request go straight to that authenticator. If this option is not checked, the request will go through authenticators in the order configured by the administrator

The use of this option does not require that the user inform an authenticator name. It is optional. If the user decides not to specify an authenticator, the authentication will happen in the usual sequence

To illustrate the domain specification, let us use a system with two configured authenticators (called *Unix* and *Windows server*). In this system, if a user called *administrator* wants to be authenticated in the *Windows server* host, the login or username should be ***administrator/Windows server***. If the suffix is not specified, the firewall will try to authenticate the user, initially through the *Unix* authenticator. If there is no user registered with this name in the *Unix* database or the ***Allow user-specified domain*** **option** is set, the firewall will then try to authenticate the user through the *Windows server* authenticator

The authenticator's name informed by the user must be in the list of firewall Authenticators that will be queried.

Authenticators to query

To add an authenticator in the Authenticators to query list, follow the steps bellow:

1. Right-click anywhere in the Authenticators to query panel or drag an Authenticator entity from the Entities list to this same place;

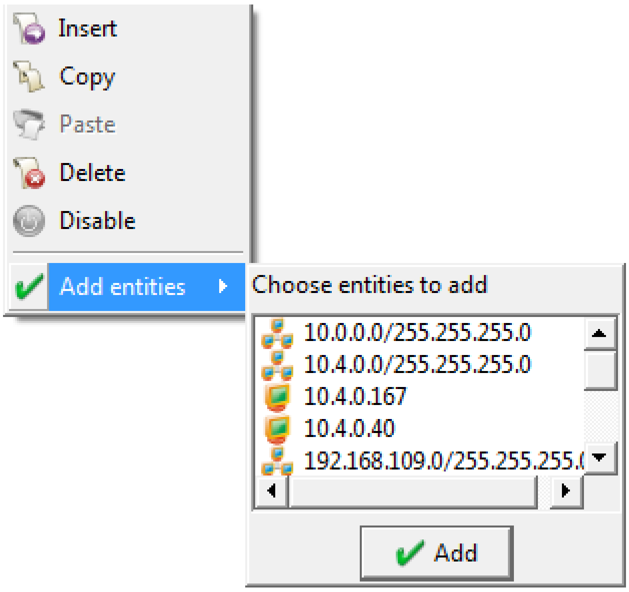

Insert
Copy
Paste
Delete
Disable
Add entities
Choose entities to add
10.0.0.0/255.255.255.0
10.4.0.0/255.255.255.0
10.4.0.167
10.4.0.40
192.168.109.0/255.255.255.(
Add

Image 374 – Access authentication: Adding entities.

2. Choose the **Add entities** option and select the authenticator to be added in the list.

To delete an authenticator from the Authenticators to query list, follow the steps below:

1. Select the authenticator to be deleted, and press delete in the keyboard, or
2. Right-click over it, and select Delete in the opened menu.

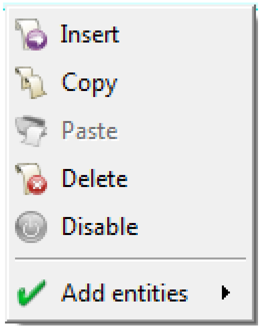

Insert
Copy
Paste
Delete
Disable
Add entities

Image 375 – Access authentication: Delete entities.

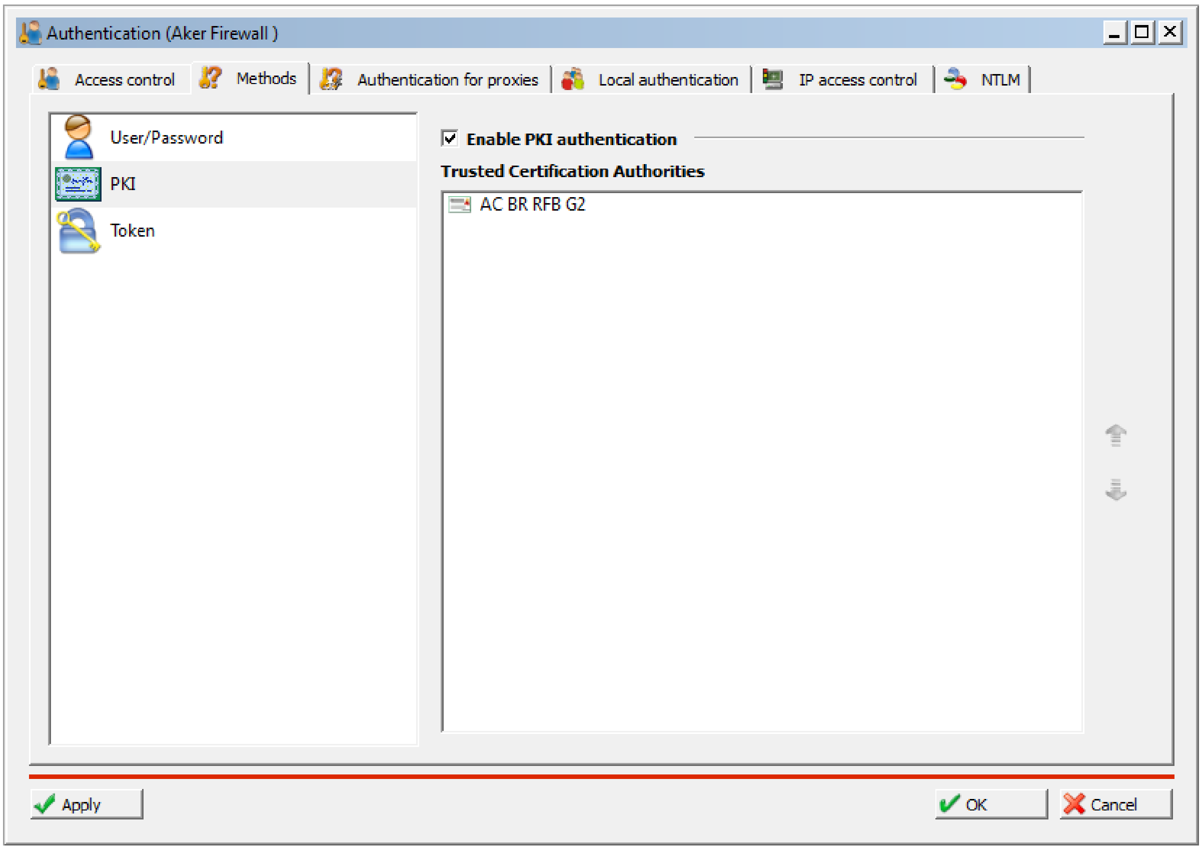
To change the query order of the authenticators, follow the steps below:

1. Select the authenticator that will have its query order position changed.
2. Click on one of the arrows on the right side of the list. The up arrow will move the authenticator up one position on the list. The down arrow will move it down one position.

Hint: It is possible to directly add and delete authenticators by drag and dropping them on the corresponding window.

The authenticators will be searched in the listed order, from top to bottom.

Enable PKI authentication: This option indicates if the firewall will accept or not the user's authentication via smart cards. If it is active, you have to configure the certificate authorities which the firewall trusts.


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
User/Password
PKI
Token
Apply
OK
Cancel

☑ Enable PKI authentication

Trusted Certification Authorities

AC BR RFB G2

Image 376 – Access authentication: Method 1.

Trusted Certification Authorities

To add a Certificate Authority in the Trusted Certification Authorities list, follow the steps below:

1. Right-click on the option **Add Entities;**
2. Select the authority you wish to add;
3. Click on **Add;**
4. You also can click on the authority and drag it to the desired position.

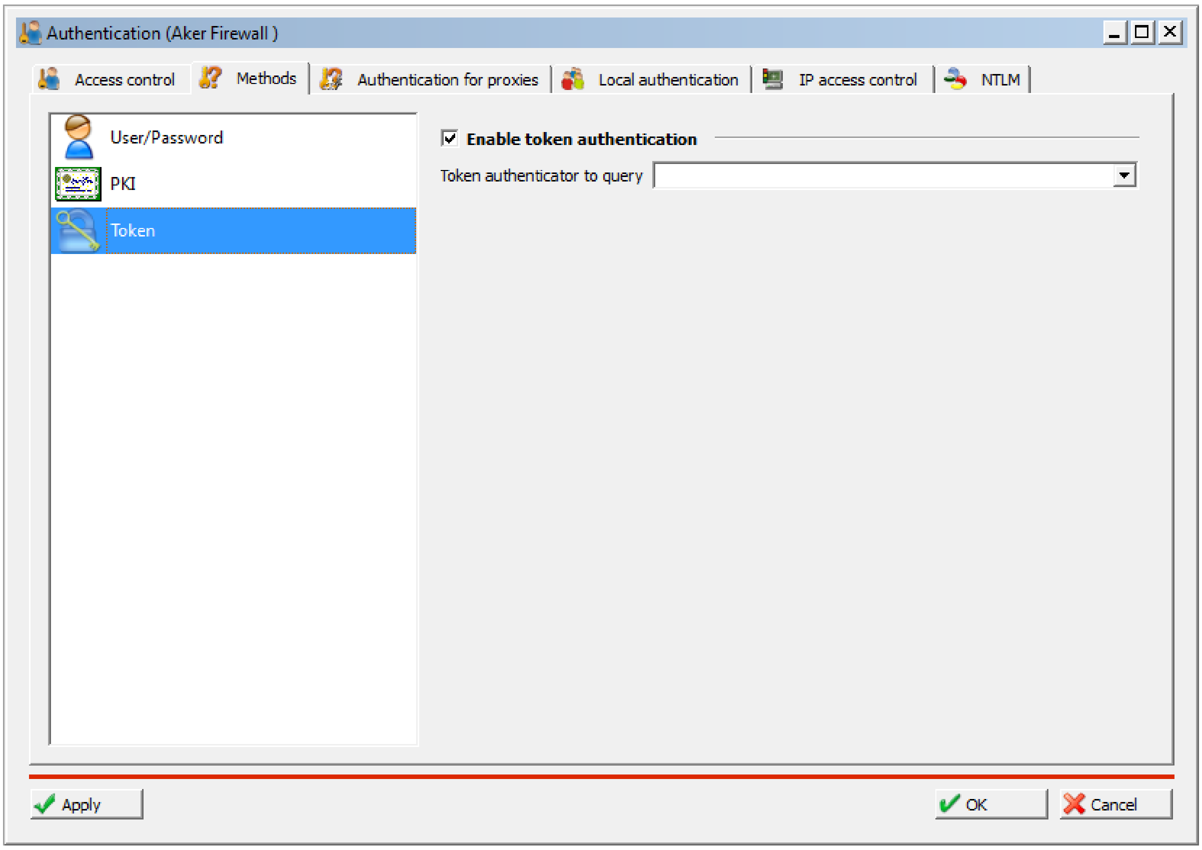
To remove a certificate authority from the *Trusted Certification* Authorities list, follow the steps below:

1. Select the authority you wish to remove and press delete on your keyboard

   or

2. Right-click on the entity you wish to remove and select the option **Delete**

Enable token authentication: This option indicates if the firewall will accept or not the user's authentication via tokens. If it is active, you have to configure the token authenticator's name selected to validate the received data.


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
User/Password
PKI
Token
Apply
OK
Cancel

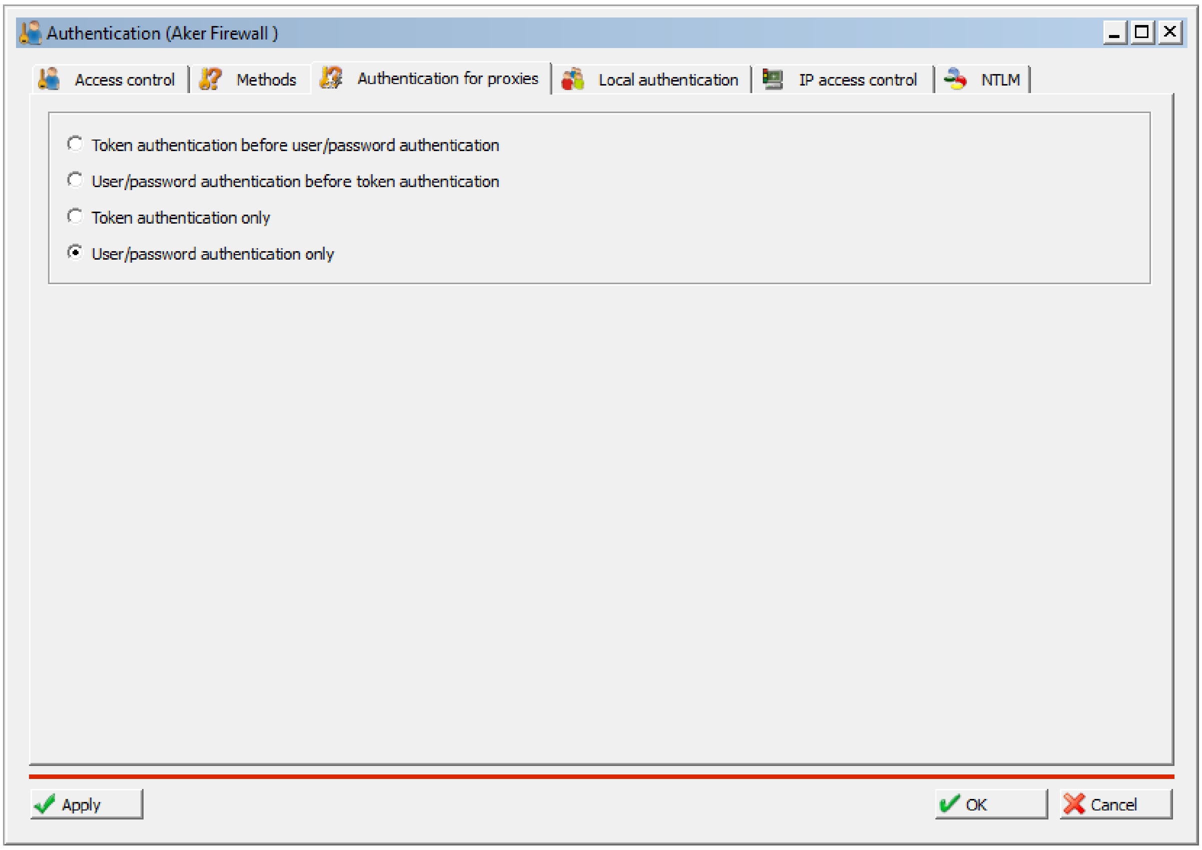
☑ Enable token authentication

Token authenticator to query

Image 377 – Access authentication: Enable token authentication method.

Token authenticator to query: This field indicates the token authenticator which the data selected to be validated will be transferred to.

Authentication for proxies tab



Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

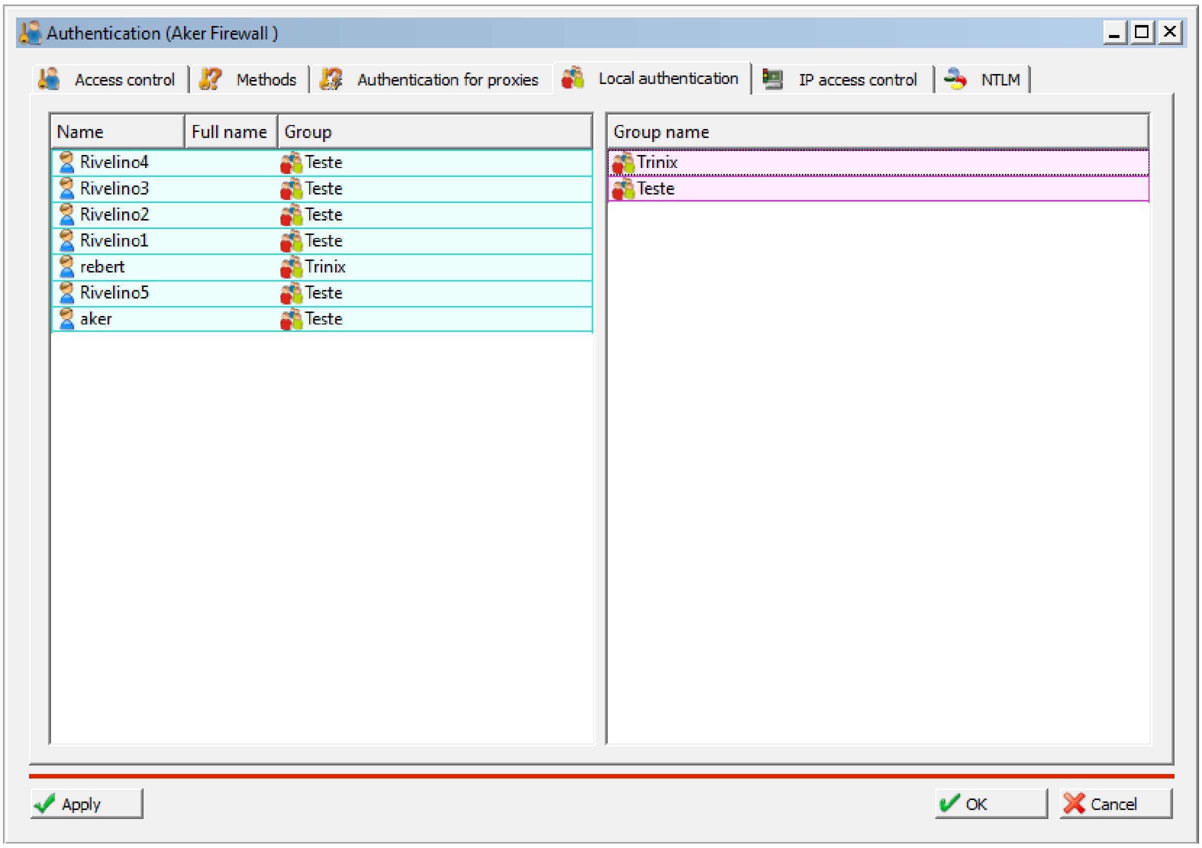
○ Token authentication before user/password authentication
○ User/password authentication before token authentication
○ Token authentication only
● User/password authentication only

Image 378 –Access authentication: Authentication for proxies.

These parameters indicate what types of authentication will be accepted by proxies and in which order they will be validated. This is important because when a user is authenticated through a browser, as example, it is not possible to specify if he is using a token or user/password. The possible options are:

- Toke authentication before user/password authentication;
- User/password authentication before token authentication;
- Token authentication only;
- User/password authentication only;

Local authentication tab


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

Name	Full name	Group
Rivelino4		Teste
Rivelino3		Teste
Rivelino2		Teste
Rivelino1		Teste
rebert		Trinix
Rivelino5		Teste
aker		Teste

Group name
Trinix
Teste

Image 379 – Access authentication: Local authentication.

In this tab, you can register several users and assign a group for each one of them.

To add a user, right-click and select the option **Insert,** or use the toolbar and click on **Insert.** You also can use the **Insert** key on your keyboard.

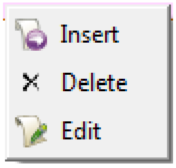
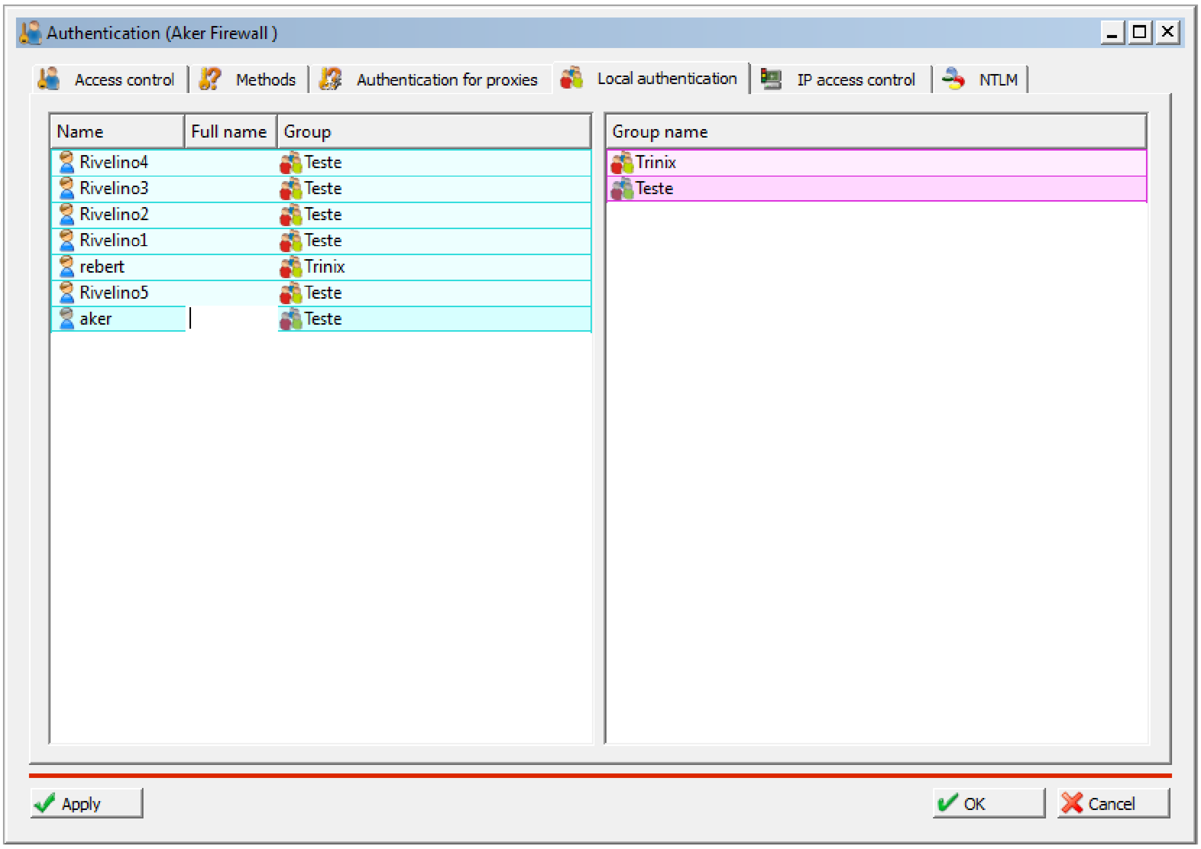

Insert
Delete
Edit

Image 380 – menu option.

To change a user name, simply double click on the corresponding field:


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

Name	Full name	Group
Rivelino4		Teste
Rivelino3		Teste
Rivelino2		Teste
Rivelino1		Teste
rebert		Trinix
Rivelino5		Teste
aker		Teste

Group name
Trinix
Teste

Image 381 – Authentication – Local authentications.

To change a password or group which is assigned to a user, right-click on the selected user and the Image bellow will be displayed:

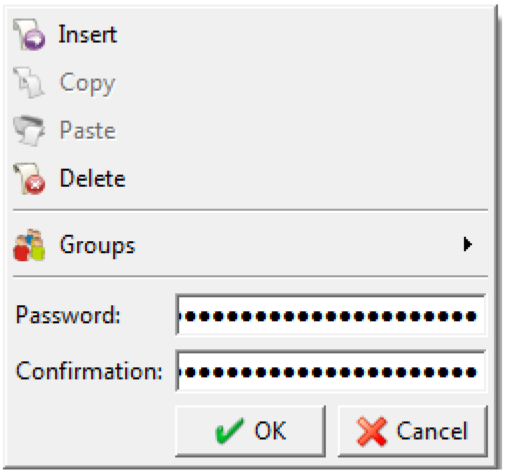
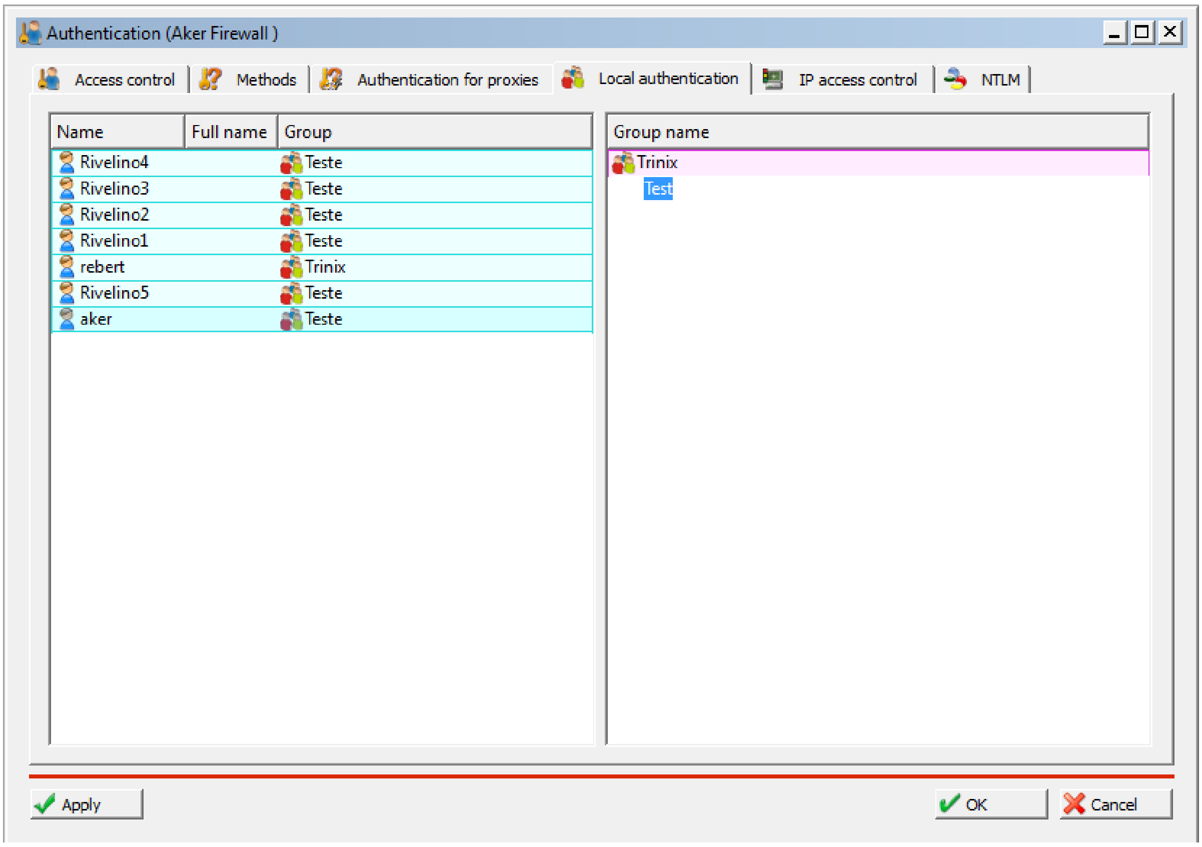

Insert
Copy
Paste
Delete
Groups
Password:
Confirmation:
OK
Cancel

Image 382 – Authentication (Changing password or group).

Creating and removing groups require the same procedure, but it is done in the Group name list.


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

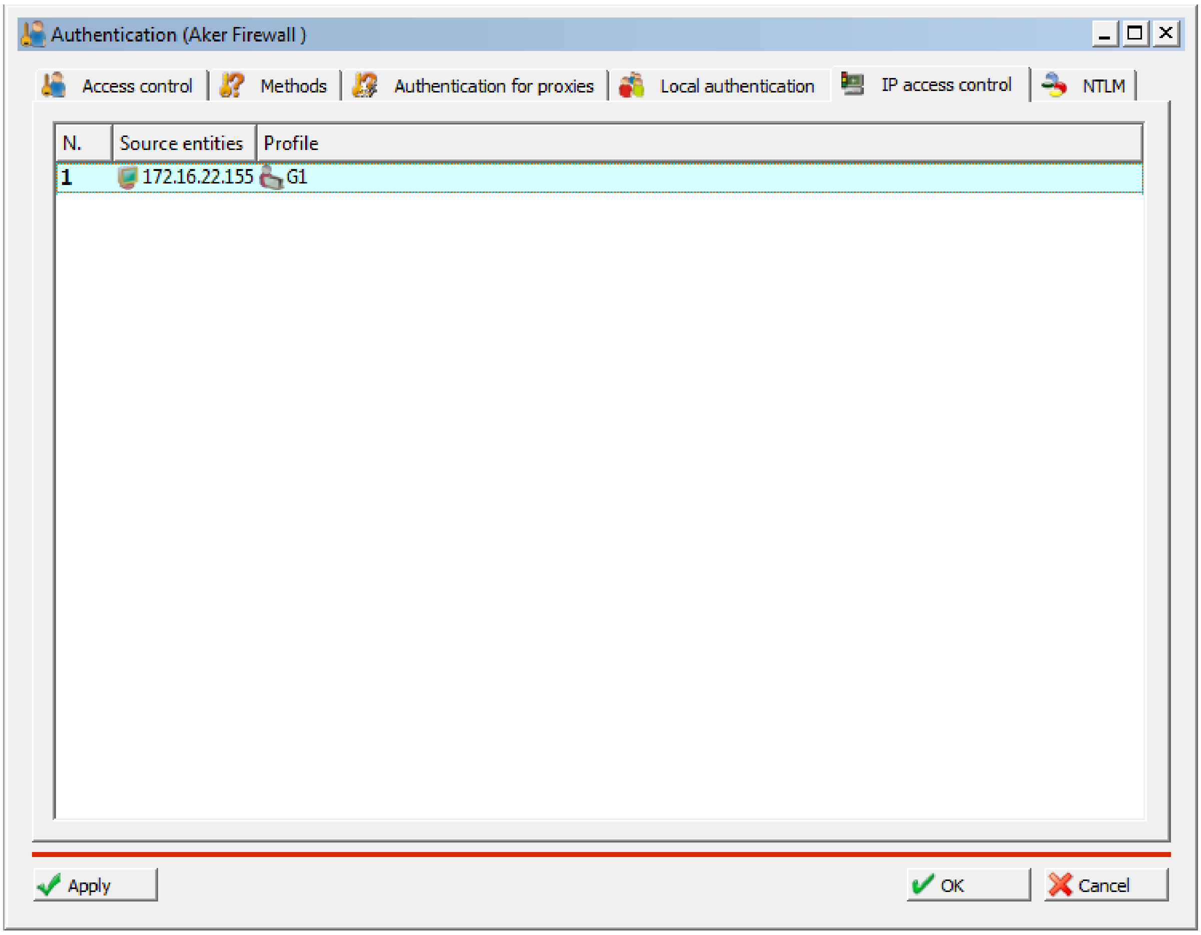
Name	Full name	Group
Rivelino4		Teste
Rivelino3		Teste
Rivelino2		Teste
Rivelino1		Teste
rebert		Trinix
Rivelino5		Teste
aker		Teste

Group name
- Trinix
  - Test

Image 383 – Local authentication – Create or delete groups.

Empty groups will not be kept by the firewall, only the ones containing at least one user.

IP access control tab


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

N.	Source entities	Profile
1	172.16.22.155	G1

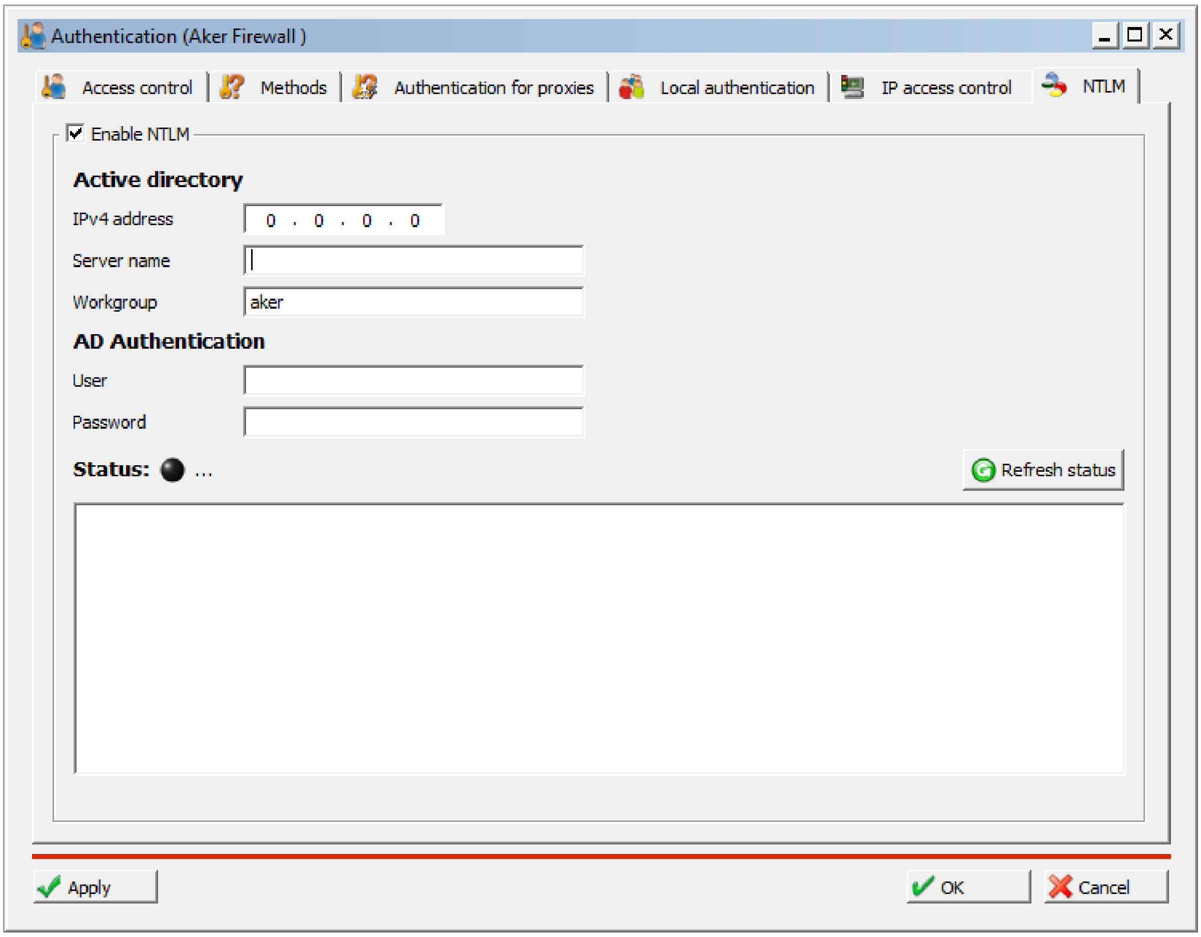
Image 384 – Ip access control via IP.

Aker Firewall can control the access using the IP addresses together with the profiles created for this end. This tab allows enabling or disabling the rules that configure the authentication through IP, so in order to disable these rules you do not have to delete them, you can enable or disable them using the menu option or use the button ⏻ which is located in the toolbar.

It is necessary to choose a network entity or a host entity that will define the traffic source and assign them to the profile, so that the traffic source of these entities do not need of authentication per user.

The access through IP will be enabled whenever there is at least one rule enabled in this tab.

NTLM tab


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Active directory
Server name
AD Authentication
User
Password
Status: ● ...
Refresh status
Apply
OK
Cancel

☑ Enable NTLM

IPv4 address 0 . 0 . 0 . 0

Workgroup aker

Image 385 – NTLM configuration.

The window above configures the Aker Firewall integration to Microsoft Active Directory (AD) and uses the automatically login without requesting the user to open the browser.

This integration is performed through Kerberos, Winbind and Samba and this authenticator behavior will be similar to other types of authentications supported by Aker Firewall, being able to list users and groups for the linking with the access profiles.

Enable NTLM: activating this option, an entity named NTLM_Auth, will be available for configuration in the *Methods tab* of the authentication window.

Active directory:

IPv4 address: Server IP address with the Microsoft Active Directory;

Server name: Server netbius name with the Microsoft Active Directory, got from the command hostname executed in this server.

AD authentication

User: User with domain admin privileges for the integration.

Password: User password.

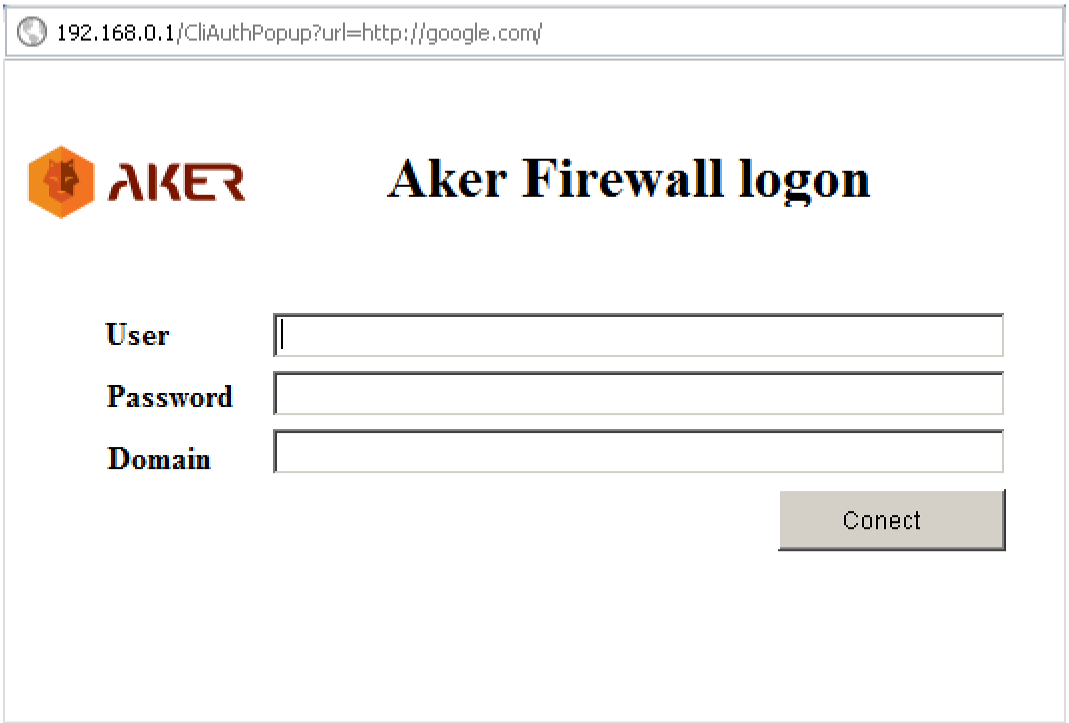
Status/Refresh status: Informs the integration status and logs in case of failures.

For better perfomance of the integration with Aker Firewall and the server with Microsoft Active Directory the date and time must to be synchronized through a NTP server.

In order to make the integration work properly the domain configured in Aker Firewall located in the System configuration window, TCP/IP, DNS tab, must to use the same domain used for the Microsoft Active Directory.

This integration is available only for the Web Filter, in the following versions the integration will be available for all functions of Aker Firewall.

Users who do not be registered in the Microsoft Active Directory domain, the authentication will be performed through a POP-UP in the user's browser. Below follows the image that will be presented to users:



192.168.0.1/CliAuthPopup?url=http://google.com/

Aker Firewall logon

Image 386 – Windows security – User and password request.

The transparent authentication will be available on for the Web Filter and the PROXY ACTIVE MODE, in the following versions the integration will be available for all functions of Aker Firewall.

22.2. Using the text interface

The Text Interface allows configuring what type of authentication will be performed and the order of the authenticators query.

Program location: */etc/firewall/fwauth*

Syntax:

```
Usage: fwauth [show | help]
       fwauth [enable | disable]
       fwauth [add | remove] [ca | token | authenticator] <entity>
       fwauth [domain | query_all] [yes | no]
       fwauth proxy [token | password] [yes | no]
       fwauth proxy first [token | password]
```

Program help:

```
Aker Firewall – Version 5.0
fwauth – Configures authentication parameters.
Usage: fwauth [show | help]
       fwauth [enable | disable]
       fwauth [add | remove] [ca | token | authenticator] <entity>
       fwauth [domain | query_all] [yes | no]
       fwauth local [first | last| no]
       fwauth proxy [token | password] [yes | no]
       fwauth proxy first [token | password]

       show          = displays current configuration
       help          = displays this message
       enable        = enables the authentication

       disable       = disables the authentication
       add           = adds an entity to the active authenticators list
       remove        = removes an entity from the active authenticators list
       domain        = enables user specified domains
       query_all     = queries all registered authenticators
       proxy password = enables user/password authentication for proxies
       proxy token   = enables token authentication for proxies
       proxy first   = specifies the first authentication method to be used
```

Example 1: (showing authentication parameters)

```
#fwauth show
AUTHENTICATION USER/PASSWORD
-----------------------------
Query all authenticators: yes
User can specify domain: no
Registered authenticators:
aut_local


PKI AUTHENTICATION
-------------------
There are no registered authenticators

TOKEN AUTHENTICATION
-----------------------
There are no registered authenticators
```

Example 2: (adding an authenticator to the active authenticators list)

```
#fwauth add authenticator "agent 10.0.0.12"
Authenticator added
```

Users access profile

23. Users access profile

This chapter shows what is for and how to configure the access profiles in Aker Firewall.

23.1. Planning the installation

What are access profiles?

Traditional firewalls base their protection rules and access controls in hosts, through their IP addresses. Aker Firewall allows this kind of control, and Aker Firewall also allows the definition of access controls based on users. This way, it is possible for certain users to have their privileges and restrictions enforced, regardless of which host they are using at a given moment. This offers the maximum flexibility and security.

To allow this user level access control, Aker Firewall has introduced the concept of access profiles. Access profiles represent the rights to be given to a specific user at the firewall. These access rights cover all firewall supported services, WWW (WORLD WIDE WEB) pages control and access control through the SOCKS proxy. This way, from a single place, it is possible to define exactly what can and cannot be accessed.

How does Access Profiles Control work?

In order to use the access profiles, initially it is necessary to create the desired profiles, and after this is, the profiles are associated with users or groups from one or more authenticators. From now on, every time a user is logged on the firewall with *Aker Client* or any other product that offers equal functionality, the firewall will identify the corresponding access profile and configure the access permissions according to this profile. Everything is performed transparently to the final user.

To make the use of access profiles possible, it is necessary to have Aker Client installed in all client hosts, or use Java authentication in the Web Filter. Otherwise, it will only be possible to use the WWW (WORLD WIDE WEB) pages access control and SOCKS proxy access control. The user authentication through WWW and SOCKS proxies is possible since they ask for a username and a password and search for the corresponding profile when they do not identify an active session for a specific host.

23.2. Registering access profiles

The access profiles define which WWW (WORLD WIDE WEB) pages can be viewed and which type of services can be accessed. Also for each WWW page or service, there is an associated timetable which is possible to define specific hours when the service or page that can be accessed.

To access the access profile window, follow the steps below:

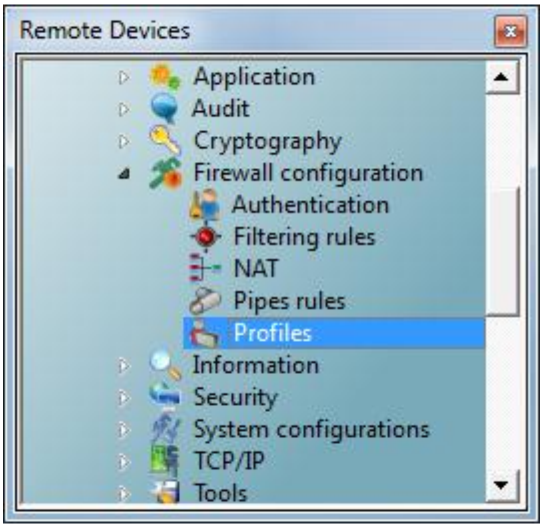
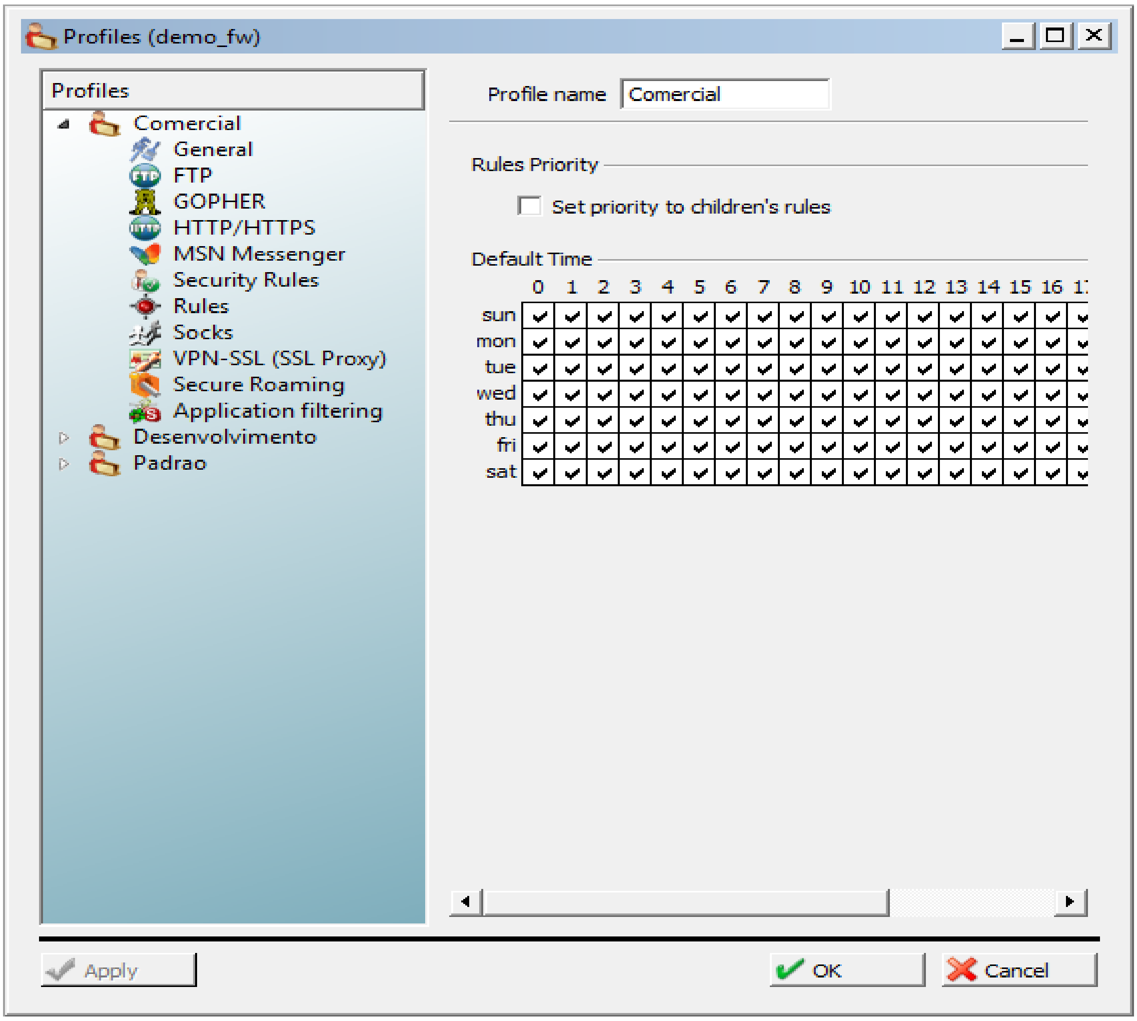

Remote Devices
Application
Audit
Cryptography
Firewall configuration
Authentication
Filtering rules
NAT
Pipes rules
Profiles
Information
Security
System configurations
TCP/IP
Tools

Image 387 – Access Profile: Profile.

- Click on the *Firewall Configuration menu*.
- Select *Profile*.

Profile window


Profiles (demo_fw)
Profiles
Comercial
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Desenvolvimento
Padrao
Rules Priority
Default Time
Apply
OK
Cancel

Profile name: Comercial

☐ Set priority to children's rules

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
sun	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
mon	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
tue	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
wed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
thu	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
fri	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Image 388 – Profiles – Aker Firewall.

The Profiles Window contains all access profiles defined in the Firewall Aker. It has a list where each profile is displayed on a separate line.

- The **OK** button will close the Profiles window.
- The **Apply** button saves all changes to the firewall and keeps the window open.

To perform any operation on a specific profile, just click on it, and then click on the corresponding option in the toolbar. The following options will be available:

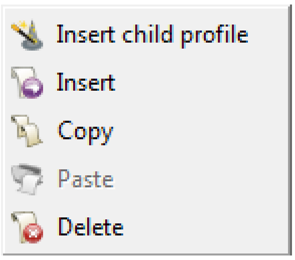


Image 389 – Profile configuration window

- **Insert child profile (sub profile)**: Inserts a new profile inside the profile that you are accessing, the new profile will be referred as *child profile* and the main profile will be referred as *father profile*, i.e., establishes a profile hierarchy.
- **Insert:** Adds a new profile in the list.
- **Copy:** Copies the selected profile.
- **Paste:** Pastes the copied profile to the desired location.
- **Delete**: Removes the selected profile from the list.
- **Profiles report:** Generates a report of the profile list in a HTML document.

Tip: All options above can be accessed in the toolbar. In the Profiles report option, first you have to select all item you want to generate a report of, and then you click on **Create.**

The use of special characteres (soaces, dashes, symbols,accents, quotes and etc..) in the creation of ***"Access Profiles"*** is not recommended

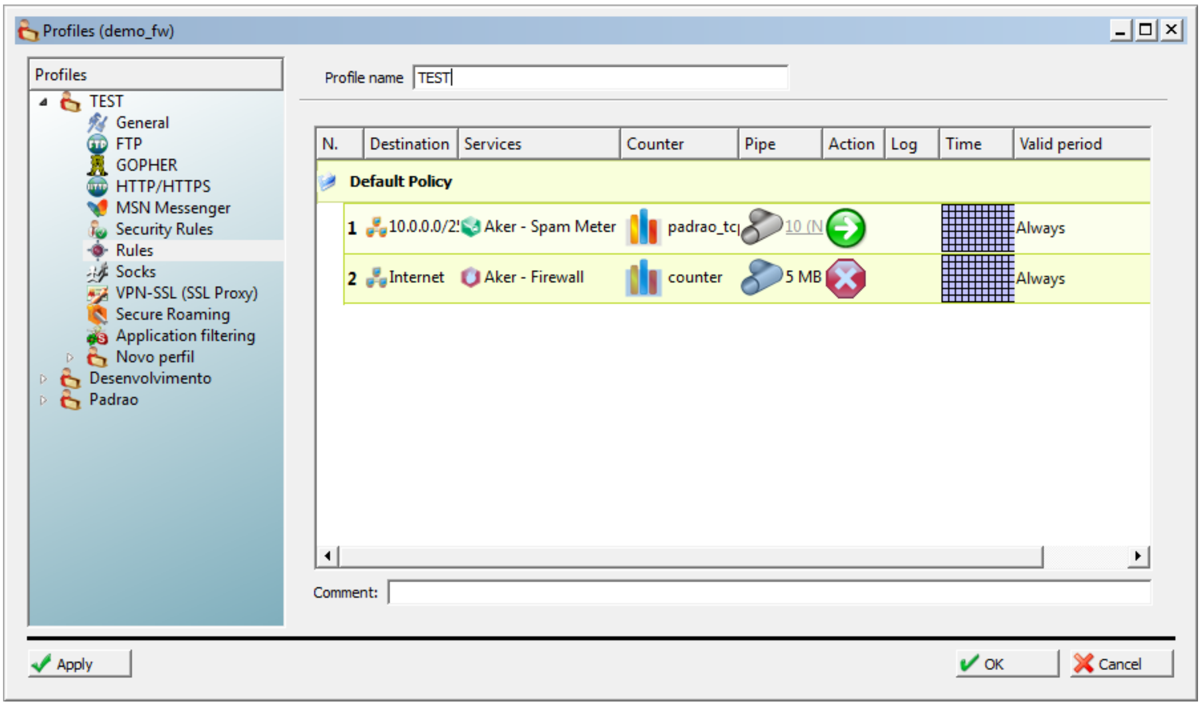
In order to delete an Access profile, it must not be assigned any user (for more information see the topic ***Assigning Users with Access Profiles)***

The child profile (subprofile) will inherit the configuration of its father profile (main profile). automatically, and you can set specific configuration for each child profile, but remember that the father profile configuration will be the main configuraiton for all child profiles.

In the upper part of the window, there is the field **Name**, used to specify the name that will uniquely identify the access profile. This name will be displayed in the profiles list and in the access control window. There may not be more than one profile with the same name.

Each access profile is composed of eleven different topics. Depending on what topic is selected at a given moment, the right part of the window will change according to the topic you have selected.

23.3. Rules



Profiles (demo_fw)

Profiles
- TEST
  - General
  - FTP
  - GOPHER
  - HTTP/HTTPS
  - MSN Messenger
  - Security Rules
  - Rules
  - Socks
  - VPN-SSL (SSL Proxy)
  - Secure Roaming
  - Application filtering
  - Novo perfil
- Desenvolvimento
- Padrao

Profile name: TEST

N.	Destination	Services	Counter	Pipe	Action	Log	Time	Valid period
Default Policy								
1	10.0.0.0/2	Aker - Spam Meter	padrao_tc	10 (N	➔		▦	Always
2	Internet	Aker - Firewall	counter	5 MB	✗		▦	Always

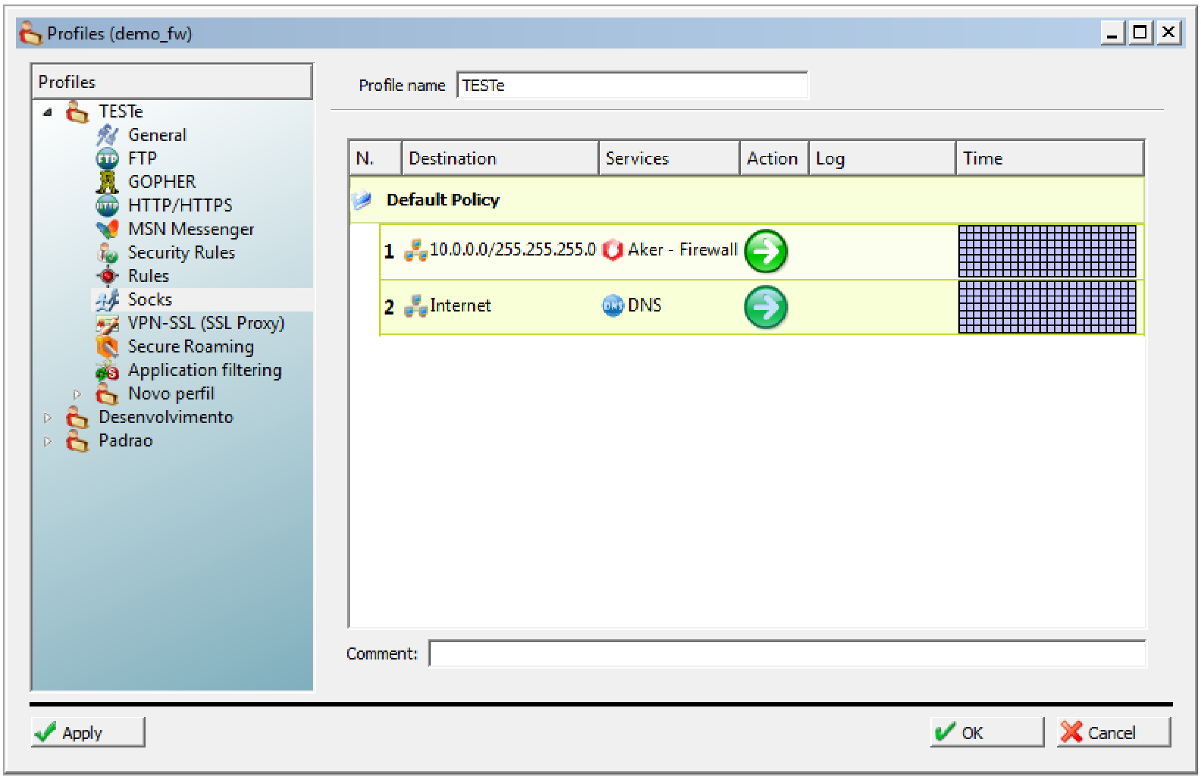
Comment:

Image 390 – Rules: Access profile filtering rules.

Access profile filtering rules are specified in the Rules Tab. This tab's format is exactly the same as the Filtering Rules Window, except that in this case, it is not required to specify source entities (for more information, check the chapter titled **Stateful Filter**).

Access profile filtering rules consider as the source, the host in which the session was established. Thus, it is only necessary to specify the destination entities and the services that can be accessed.

23.4. SOCKS rules


Profiles (demo_fw)
Profiles
TESTe
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Novo perfil
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: TESTe

N.	Destination	Services	Action	Log	Time
Default Policy					
1	10.0.0.0/255.255.255.0	Aker - Firewall	→		
2	Internet	DNS	→		

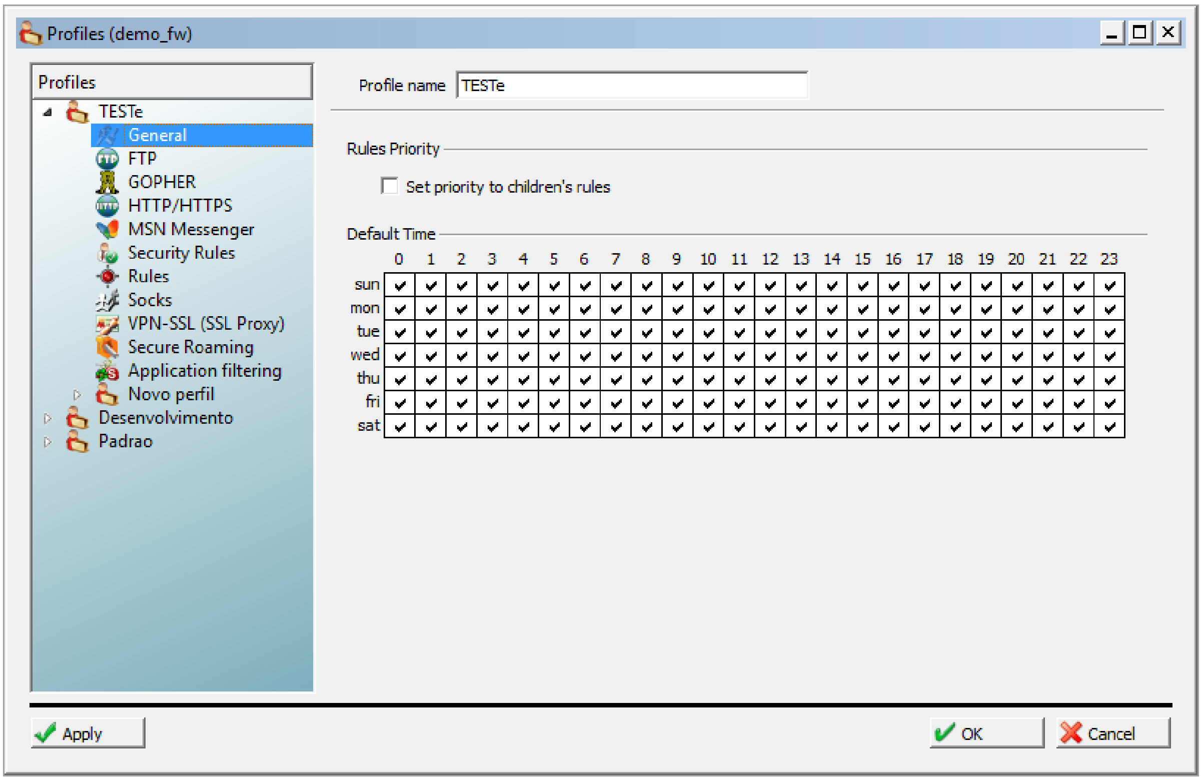
Comment:

Image 391 – Profile: Socks.

The SOCKS Rules Tab allows the configuration of filtering rules for SOCKS proxy access. It has the same format as the Filtering Rules window, except that it is not required to specify a source entity (for more information, see the chapter titled **Stateful Filter**).

SOCKS proxy filtering rules consider as source the host in which the session was established. Therefore, it is only necessary to specify the destination entities and the services that may be accessed.

23.5. General


Profiles (demo_fw)
Profiles
TESTe
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Novo perfil
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: TESTe

Rules Priority

☐ Set priority to children's rules

Default Time

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
sun	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
mon	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
tue	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
wed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
thu	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
fri	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
sat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Image 392 – Profile: General.

The general filtering options are defined by the following fields:

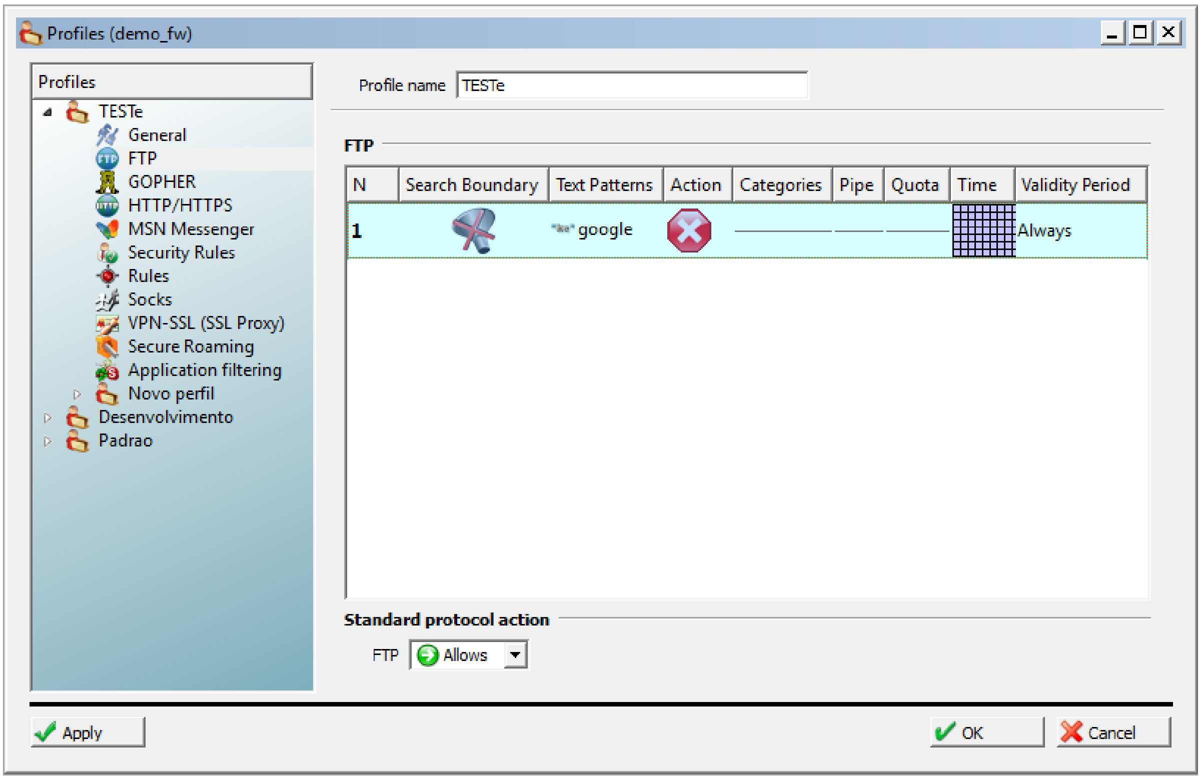
Rules Priority: Allows defining the priority between the profile rules and the rules of its children's profile.

- **Set priority to children's rules:** If this option is checked, the children's (sub profiles) profile rules will be above the father's (main profiles) profile rules, i.e. the children's rules will have priority over the father's rules. Otherwise, if this option is not checked the father's profile rules will priority.

- **Default time:** This table defines WWW (WORLD WIDE WEB) filtering rules default schedule. After adding WWW filtering rules, it is possible to choose between using this default timetable and specifying a different time.

  Rows represent weekdays, and the columns represent the time of the day. To apply the rule at a specific time of the day, check the box beneath it, on the row of the desired day of the week. Otherwise, leave it blank. To make the configuration easier, you may click on a square and drag the mouse over squares you want to check/uncheck, while keeping the button pressed. The table will be altered as the mouse moves over the cells.

23.6. FTP and GOPHER


Profiles (demo_fw)
Profiles
TESTe
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Novo perfil
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: TESTe

FTP

N	Search Boundary	Text Patterns	Action	Categories	Pipe	Quota	Time	Validity Period
1		google						Always

Standard protocol action

FTP: Allows

Image 393 – Profiles: FTP and Gopher.

The option FTP and GOPHER filtering allow the definition of rules of URLs' filtering for the FTP and GOPHER protocol. It consists of a list where each rule is displayed in a separated line.

At bottom part of the window, there is a group that defines the action to be performed in case the target's address does not match any filtering rule. This group is called **Standard Protocol Action** and it has two options for each protocol:

Allows: The firewall will accept all URLs that do not match any rule.

Blocks: The firewall will reject all URLs that do not match any rule.

Bellow follows the available options:

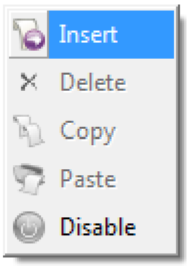


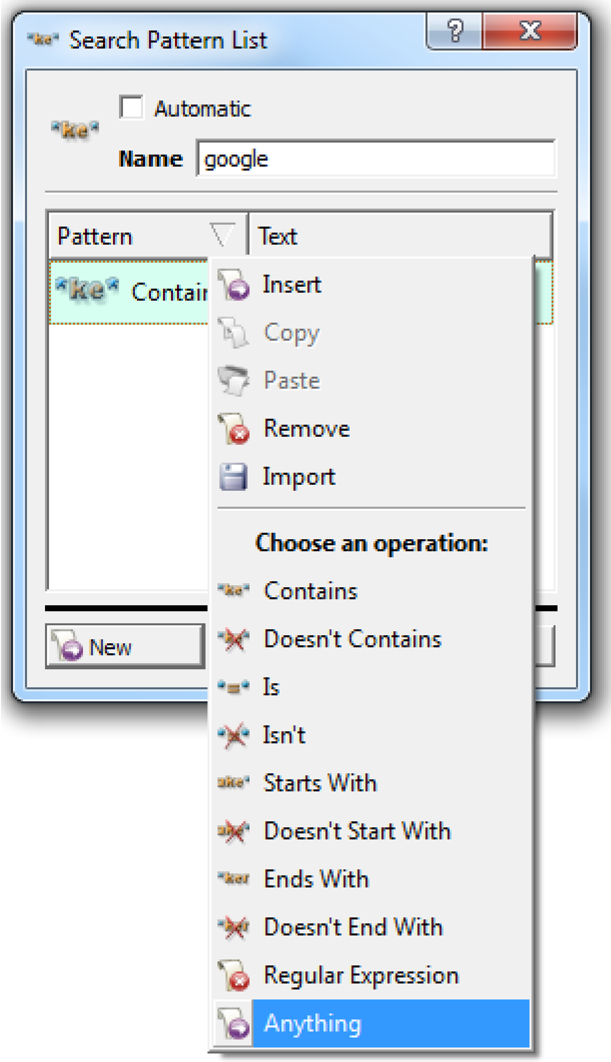
Image 394 – Access profile window (Insert and disable).

- **Insert:** This option adds a new rule to the list. If any existing rule is selected, the new one will be inserted in its position on the list, pushing it down. Otherwise, the new rule will be included at the end of the list.
- **Delete:** Removes the selected rule from the list.
- **Copy:** Copies the selected rule to a temporary area.
- **Paste:** Copies the rule from the temporary area into the list. If any existing rule is selected, the new one will be copied into its position. Otherwise, it will be copied to the end of the list.
- **Disable:** Activate or deactivate a selected rule in the list.

Hint: A rule position can be changed by dragging and dropping it at the desired position.

The order of the filtering rules is extremely important. When the firewall receives an address connection request, it researches the list from the beginning, looking for a matching rule for that address. As soon as one of this rules is found, the action associated to it, will be executed.

Each filtering rule consists of an operation, which indicates the type of search that will be performed, and the text that will be searched. The following operation options will be available:



Search Pattern List

☐ Automatic

Name google

Pattern
Text
Contai
Insert
Copy
Paste
Remove
Import
Choose an operation:
Contains
Doesn't Contains
Is
Isn't
Starts With
Doesn't Start With
Ends With
Doesn't End With
Regular Expression
Anything
New

Image 395 – Operation options.

- **CONTAINS:** The URL must contain the specified text in any position.
- **DOES NOT CONTAIN:** The URL cannot contain the specified text.
- **IS:** The URL content must be the same as the specified text.
- **IS NOT**: The URL content must be different from the specified text.
- **STARTS WITH:** The URL content must begin with the specified text.
- **DOES NOT START WITH:** The URL content must not start with the specified text.
- **ENDS WITH:** The URL content must end with the specified text.
- **DOES NOT END WITH:** The URL content must not end with the specified text.
- **REGULAR EXPRESSION:** In this case the URL will be matched against an regular expression
- **Anything:** All of the URL content will be accepted.

Below follows the definition for the options above:

N: Filtering rule number.

Search Boundary: This field allows choosing which part of the URL the search will be performed on, and the parameters that will be searched are defined in the **Text patterns**.

Text Patterns: Right-clicking on this field allows you to select a pattern entity list created previously. So it will be possible associate a rule to a pattern entity of search, allowing defining what *string* or parameter will be searched in the URL accessed and what operation will be performed.

Action: Defines the action to be performed in case the address that the user wishes to access does not fit in any filtering rule. It consists of two options:

- **Allows**: The firewall will accept the URLs that do not fit in any rule.
- **Blocks**: The firewall will reject the URLs that do not fit in any rule.

Categories: This field allows you to associate any category to the rule that is being created.

Pipe: Used in the Filtering rules with the purpose of limiting the bandwidth of certain services, hosts, networks and users.

Quota: Quotas are used to control and rationalize the time used by employees access the websites. This way the “Quotas” are the limits of the access time and the data volume.

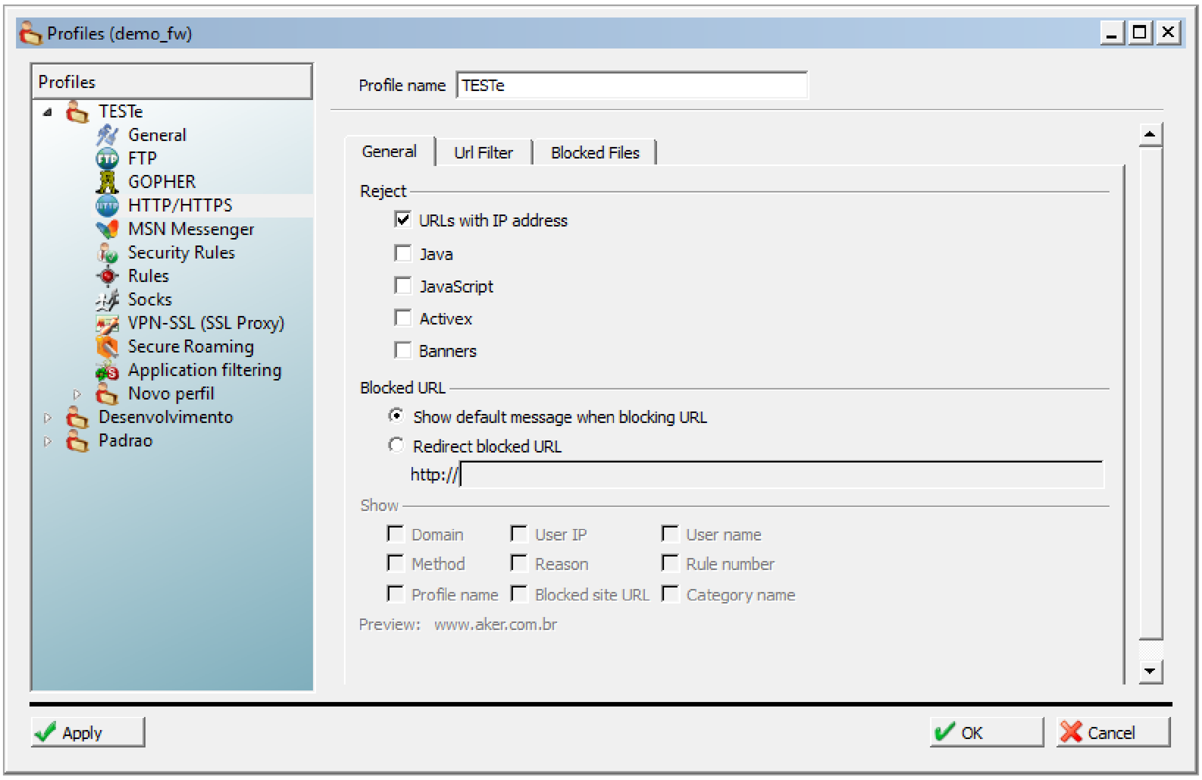
Time: The period that the rule will be applied defined on week day and time.

Example: Allow that on Mondays and Wednesdays the user will be granted access to the Internet from 12:00 to 14:00.

Validity Period: Validity period and rule application defined in month and year.

23.7. HTTP/HTTPS

General Tab


Profiles (demo_fw)
Profiles
TESTe
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Novo perfil
Desenvolvimento
Padrao
General
Url Filter
Blocked Files
Apply
OK
Cancel

Profile name: TESTe

Reject
☑ URLs with IP address
☐ Java
☐ JavaScript
☐ Activex
☐ Banners

Blocked URL
● Show default message when blocking URL
○ Redirect blocked URL
http://

Show
☐ Domain ☐ User IP ☐ User name
☐ Method ☐ Reason ☐ Rule number
☐ Profile name ☐ Blocked site URL ☐ Category name

Preview: www.aker.com.br

Image 396 – General: HTTP and HTTPS.

Block: This field defines the blocking options for WWW (WORLD WIDE WEB) sites. They are:

- **URLs with IP address:** If this option is checked, access to URLs with IP addresses will be rejected, (for example, http://127.0.0.1/index.html), while the access using URLs names will be accepted.

If the WWW proxy is configured to filter URLs, this option must also be configured to avoid access via IP address. Otherwise, even with the name blocked, the user will continue being able to access the URL via its IP address. It is possible to add IP addresses to the WWW filtering rules (if this filtering option is active). Since the IP addresses frequently change and many servers have more than one.

The URL blocking does not have support for HTTPS pages when the active Proxy is being used (when blocking a page using this method, the browser will show the communication error.

Java, JavaScript and ActiveX: This field defines a special filtering for the WWW pages, blocking or not features considered dangerous in some environments. It has three options that can be checked independently: **JavaScript**, **Java** and **ActiveX**. For each checked option, the corresponding applets will be filtered.

The filtering of JavaScript, Java and ActiveX is made in a way that the filtered page is viewed as if the client browser did not have support for the filtered languages. In some cases, this can cause the pages to lose their functionality.

- **Banners block:** This option performs the blocking of advertisement banners on web pages. If it is checked, the firewall will replace the banners for empty spaces on the pages, lowering the loading delay.

  If the blocking is active, it will be performed based on global rules, equal to all profiles. In order to configure these rules, follow the steps bellow

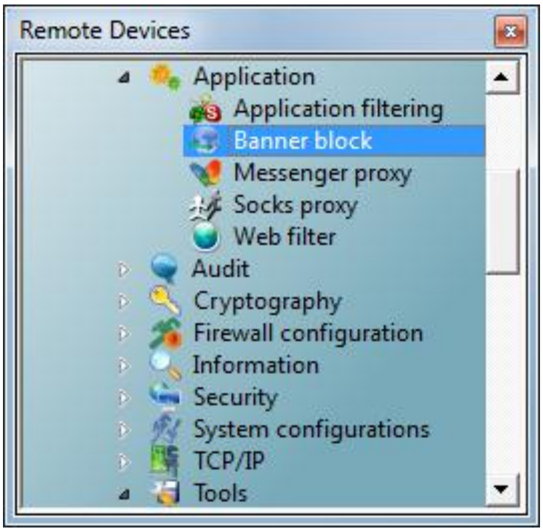
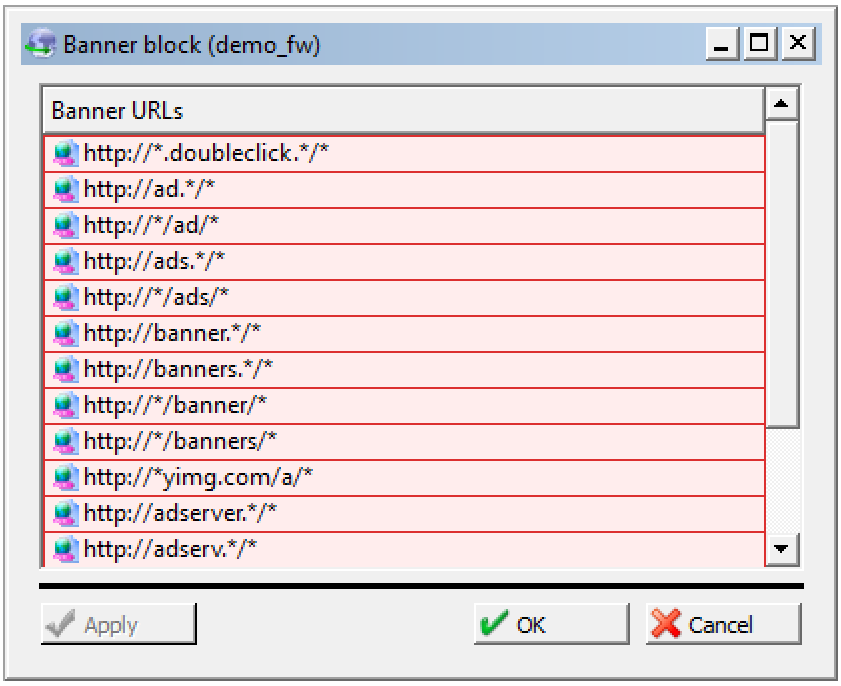

Remote Devices
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
System configurations
TCP/IP
Tools

Image 396 – access window: banner block.

- Click on the *Application menu*
- Select *Banner Block*

The following window will be displayed:



http://*.doubleclick.*/*
http://ad.*/*
http://*/ad/*
http://ads.*/*
http://*/ads/*
http://banner.*/*
http://banners.*/*
http://*/banner/*
http://*/banners/*
http://*yimg.com/a/*
http://adserver.*/*
http://adserv.*/*

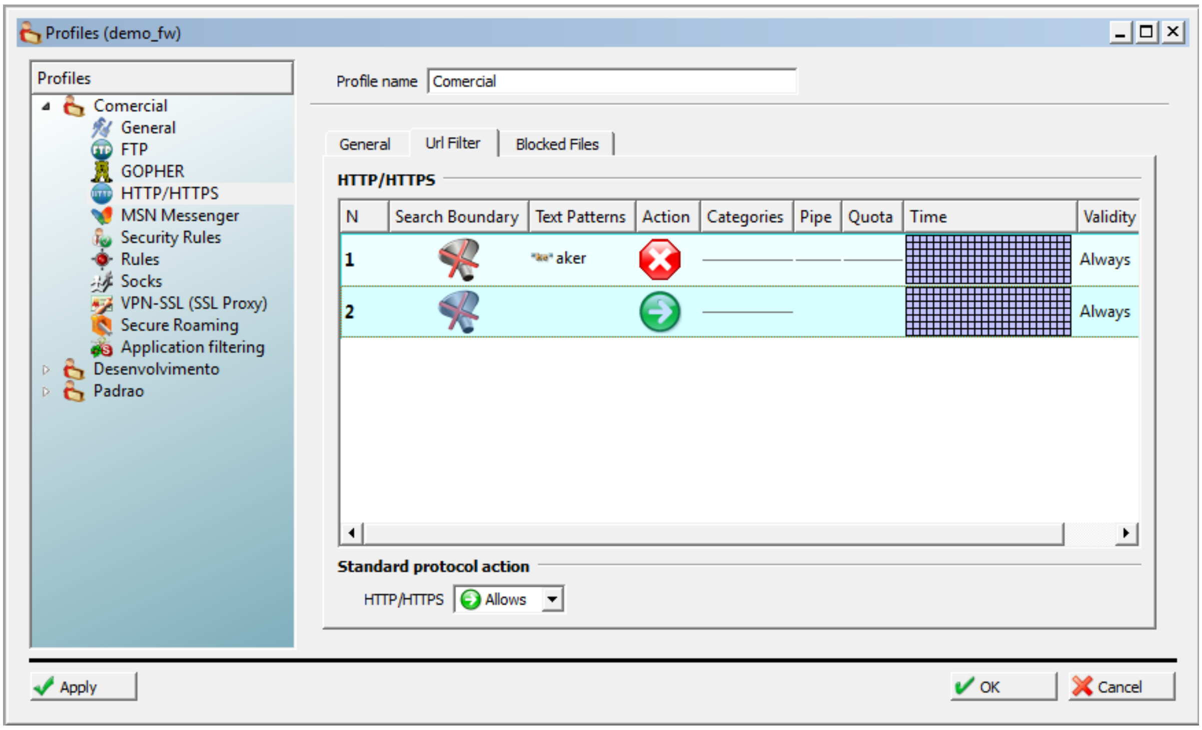
Image 397 – Banner block (Banner URLs).

This window is formed of many rules in the regular expression format. In case a URL fit in rule in the list, it will be consider as blocked.

The HTTP/HTTPS filtering tabs allows the URLs filtering rules definition to the HTTP/HTTPS protocols. It consists of a list where each rule is displayed on a separate line.

The HTTPS protocol for the initial URL is filtered, as it was the HTTP protocol. Besides it, once the communication is established the firewall will not be able to filter any part of its content, since the encryption is performed directly between the client and server.

URL Filter


Profiles (demo_fw)
Profiles
Comercial
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Desenvolvimento
Padrao
General
Url Filter
Blocked Files
Apply
OK
Cancel

Profile name: Comercial

HTTP/HTTPS

N	Search Boundary	Text Patterns	Action	Categories	Pipe	Quota	Time	Validity
1		aker	✗	——	——	——	▦	Always
2			→	——			▦	Always

Standard protocol action

HTTP/HTTPS: Allows

Image 398 – Profile: URL Filter.

In the bottom part of the window, there is a group that defines the action to be performed in case the target address does not match any filtering rule. This group is called **Standard Protocol Action** and it has two options for each protocol:

Allows: The firewall will accept all URLs that do not match any rule.

Blocks: The firewall will reject all URLs that do not match any rule.

Bellow follows the available options:

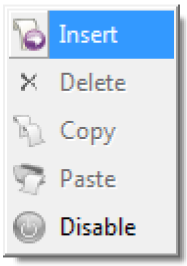

Insert
Delete
Copy
Paste
Disable

Image 399 – Toolbar (insert or disable)

- **Insert:** This option adds a new rule to the list. If any existing rule is selected, the new one will be inserted in its position on the list, pushing it down. Otherwise, the new rule will be included at the end of the list.

- **Delete:** Removes the selected rule from the list.
- **Copy:** Copies the selected rule to a temporary area.
- **Paste:** Copies the rule from the temporary area into the list. If any existing rule is selected, the new one will be copied into its position. Otherwise, it will be copied to the end of the list.
- **Disable:** Activate or deactivate a selected rule in the list.

Hint: A rule position may be altered by dragging and dropping it at the desired position.

The order of the filtering rules is extremely important. When the firewall receives an address connection request, it researches the list from the beginning, looking for a matching rule for that address. As soon as one of this rules is found, the action associated to it, will be executed.

Each filtering rule consists of an operation, which indicates the type of search that will be performed, and the text to be searched. The following operation options will be available

- **CONTAINS:** The URL must contain the specified text in any position.
- **DOES NOT CONTAIN:** The URL cannot contain the specified text.
- **IS:** The URL content must be the same as the specified text.
- **IS NOT**: The URL content must be different from the specified text.
- **STARTS WITH:** The URL content must begin with the specified text.
- **DOES NOT START WITH:** The URL content must not start with the specified text.
- **ENDS WITH:** The URL content must end with the specified text.
- **DOES NOT END WITH:** The URL content must not end with the specified text.
- **REGULAR EXPRESSION:** In this case the URL will be matched against an regular expression
- **Anything:** All of the URL content will be accepted.

Below follows the definition for the options above:

N: Filtering rule number.

Search Boundary: This field allows choosing what part of the URL the search will be performed, and the parameters to be searched will be defined in the **Text patterns**.

Text Patterns: Right-clicking on this field allows you to select a pattern entity list created previously. With this will be possible associate a rule to a pattern entity of search, allowing defining what *string* or parameter will be searched in the URL accessed and what operation will be performed.

Action: Defines the action to be performed in case the address that the user wishes to access does not fit in any filtering rule. It consists of two options:

Allows: The firewall will accept all URLs that do not match any rule.

Blocks: The firewall will reject all URLs that do not match any rule.

Categories: This field allows you to associate any category to the rule that is being created.

Pipe: Used in the Filtering rules with the purpose of limiting the bandwidth of certain services, hosts, networks and users.

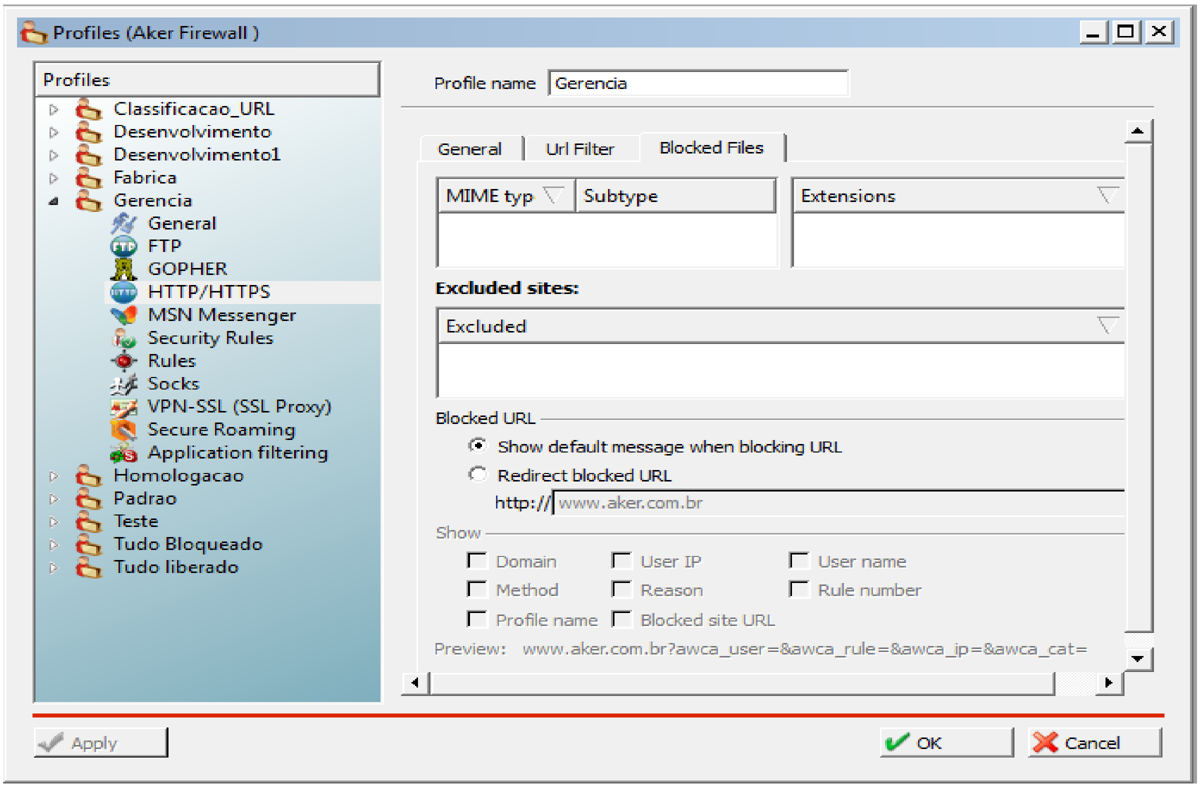
Quota: Quotas are used to control and rationalize the time used by employees access the websites. This way the “Quotas” are the limits of the access time and the data volume.

Time: The period that the rule will be applied defined on week day and time.

Example: Allow that on Mondays and Wednesdays the user will be granted access only for the Internet from 12:00 to 14:00.

Validity Period: Validity period and rule application defined in month and year.

Blocked files tab


Profiles (Aker Firewall)
Profiles
Classificacao_URL
Desenvolvimento
Desenvolvimento1
Fabrica
Gerencia
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Homologacao
Padrao
Teste
Tudo Bloqueado
Tudo liberado
General
Url Filter
Blocked Files
MIME typ
Subtype
Extensions
Excluded
Apply
OK
Cancel

Profile name: Gerencia

Excluded sites:

Blocked URL
● Show default message when blocking URL
○ Redirect blocked URL
http:// www.aker.com.br

Show
☐ Domain ☐ User IP ☐ User name
☐ Method ☐ Reason ☐ Rule number
☐ Profile name ☐ Blocked site URL

Preview: www.aker.com.br?awca_user=&awca_rule=&awca_ip=&awca_cat=

Image 400 – Profile: Blocked files.

This tab specifies the files that the profile and the Web Filter will block.

In order to decide if a transferred file needs to be blocked, you may use one of the following options: the file extension or its MIME type. If one of these options is met, the firewall will block this file.

The MIME type consists of two identifiers, the first one indicates the type and the second indicates the subtype. The browser uses this information to decide how to show the received information in the same manner that the operating system uses the file extension name.

Deleted websites:

Here you need to choose the operation and the text you are including for the analysis. Web sites that fit in the deleted list will not be analyzed.

Operation options:

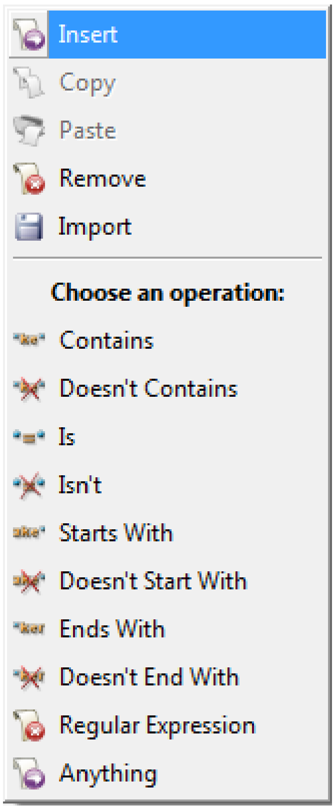

Insert
Copy
Paste
Remove
Import
Choose an operation:
Contains
Doesn't Contains
Is
Isn't
Starts With
Doesn't Start With
Ends With
Doesn't End With
Regular Expression
Anything

Image 401 – Choosing an operation.

Blocked URL:

Allows configuring what action will be taken by the firewall when a user attempts to access a blocked URL. Bellow follows the description of the options of the Blocked URL.

Show default message when blocking URL: When this option is selected the firewall shows an error message informing that the following URL has been blocked.

Redirect blocked URL: When this option is selected the firewall will redirect the attempts of access to blocked URLs to a URL selected by administrator. In this case the URL which the blocked access will be redirected must to be specified (without the http:// prefix).

Show: This option defines the page that will be displayed to user when attempting to access a blocked URL. It can be the default page or redirect to a specific page, which will be customized according to the selected check boxes.

Each check box is a parameter used to identify where and why the page was blocked, for example, if the page was blocked because it fits in any category on blocked list.

Domain: When this option is selected the URL domain will be displayed. Example: At URL www.aker.com.br, the domain would be aker.com.br. Selecting this option the *domain variable* will be created.

Method: Informs the method used by the HTTP protocol. E.g. GET, PUT, POST. When the method is selected the *method variable* will be created.

Profile name: Name given by user to the selected profile. Selecting this option the *profile variable* will be created.

User IP: User's IP address who has attempted to access the blocked URL. Selecting this option the IP *variable* will be created.

Reason: Selecting this option =- the *variable Reason* will be created. Enabling this option the reason of the website blocking will be displayed.
Bellow follows examples of reasons:

"URL category",
"Rule block",
"exceeded quota bytes",
"insufficient quota bytes "
"exceeded quota time",
"object type not allowed",
"file type not allowed globally",
"file type not allowed in the profile",
"connect for specified port not allowed"

Category name: Category name that was associated to the URL. Selecting this option the *cats variable* will be created.

User name: User name who has attempted to access the URL. Selecting this option the *user variable* will be created

Rule number: Filtering rule number that the URL has matched. Selecting this option the *rule variable* will be created.

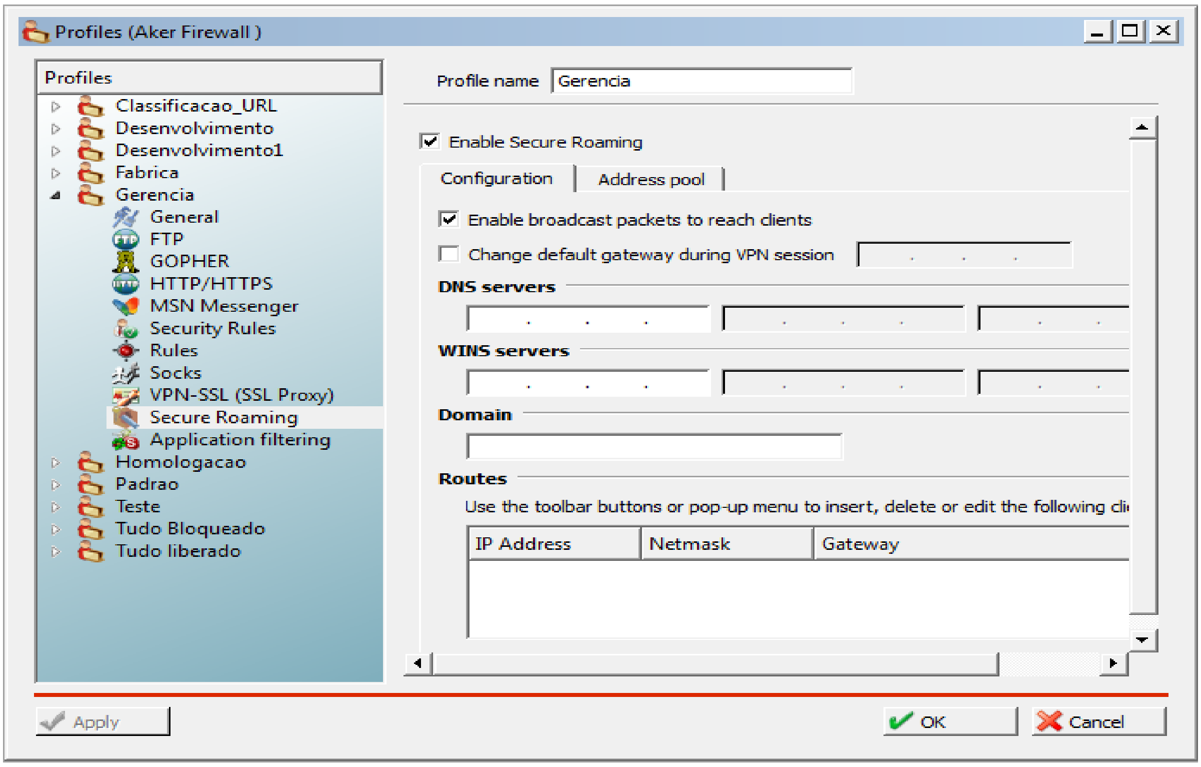
Blocked site URL: Shows the URL that the user has attempted to access and was blocked. When this option is selected the *URL variable* will be created.

When the active proxy is being used and an URL is blocked by a quota or by a default query list, the default page for blocking will not be displayed.

Preview shows the URL and what will be sent via GET method.

23.8. Secure Roaming

Configuration tab



Profiles (Aker Firewall)
Profiles
Classificacao_URL
Desenvolvimento
Desenvolvimento1
Fabrica
Gerencia
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Homologacao
Padrao
Teste
Tudo Bloqueado
Tudo liberado
Configuration
Address pool
DNS servers
WINS servers
Domain
Routes
IP Address
Netmask
Gateway
Apply
OK
Cancel

Profile name: Gerencia

☑ Enable Secure Roaming

☑ Enable broadcast packets to reach clients

☐ Change default gateway during VPN session

Use the toolbar buttons or pop-up menu to insert, delete or edit the following cli

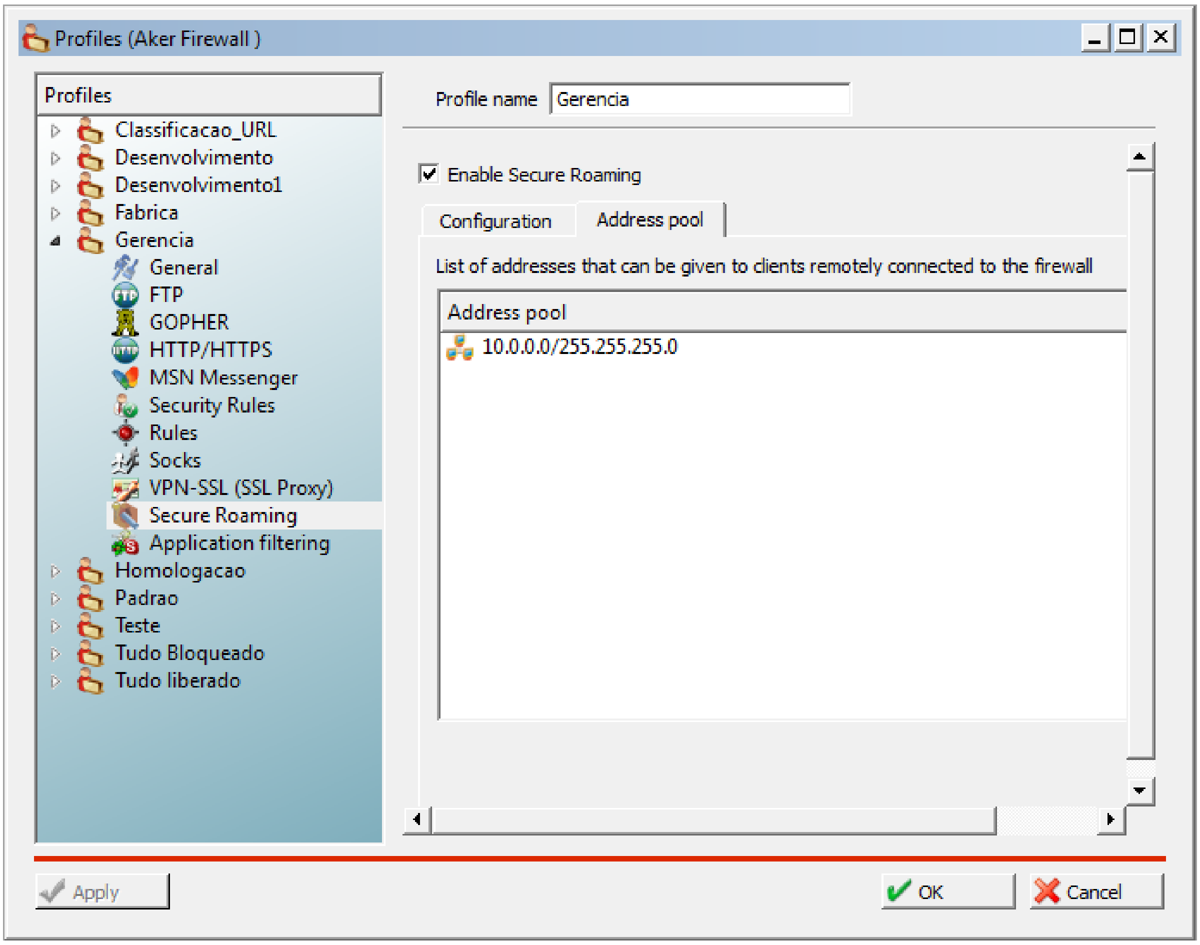
Image 402 – Profiles: Security Roaming.

This tab allows the option of Secure Roaming access that varies according with the client permissions that is connected, for more information see the chapter **Secure Roaming configuration**.

- **Enable Secure Roaming:** Enables the use of Firewall secure roaming.
- **Enable broadcast packets to reach clients:** Broadcast packets are used by protocols that need in any part of its operation a communication between hosts and all others of a sub-network in an efficient mode.
- **Change default gateway during VPN session:** When changing the *hosts default route* that connects via Secure Roaming, they will not be able to access other destination on the Internet without passing through the network with the Secure Roaming virtual addresses.

- **DNS server:** Configures up to three DNS servers which will be used during the encryption session. This is used in case there is an internal DNS server in the corporation.
- **WINS server:** Configures up to three WINS server which will be used during the encryption session. This configuration will be useful in case the corporation uses internal WINS server. It is ignored by clients who do not use Windows.
- **Domain:** Adds a domain to the configuration of client host names during the encrypted session. Normally it is used together with the DNS servers change.
- **Routes:** During the client session few routes can be need to access several services in the Intranet. They are registered in this field.

Address pool tab


Profiles (Aker Firewall)
Profiles
Classificacao_URL
Desenvolvimento
Desenvolvimento1
Fabrica
Gerencia
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Homologacao
Padrao
Teste
Tudo Bloqueado
Tudo liberado
Configuration
Address pool
Apply
OK
Cancel

Profile name: Gerencia

☑ Enable Secure Roaming

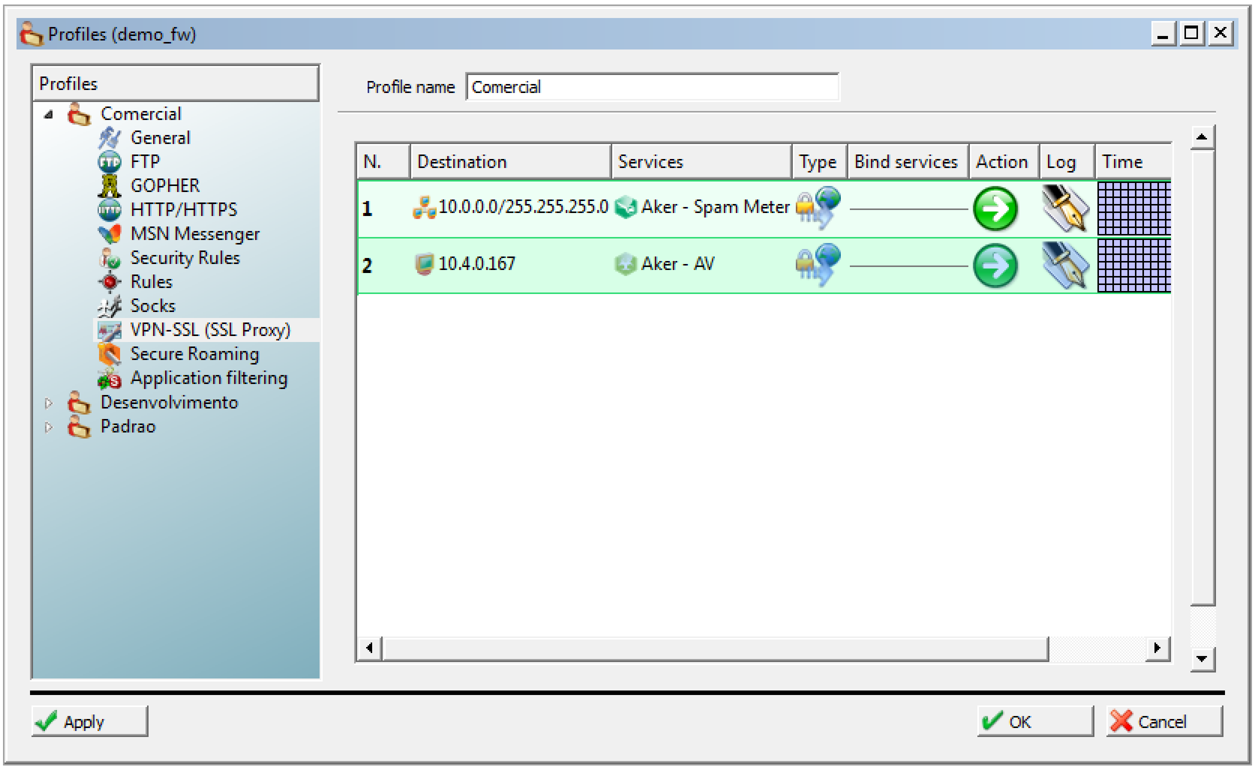
List of addresses that can be given to clients remotely connected to the firewall

Address pool
10.0.0.0/255.255.255.0

Image 403 – Profiles: Security Roaming (Address pool).

This tab defines an IP or IP range to clients who connect to the Firewall and be linked to this profile. In case there is no configuration set in this tab, the Secure Roaming default configuration will be used.

23.9. VPN SSL (Proxy SSL)


Profiles (demo_fw)
Profiles
Comercial
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: Comercial

N.	Destination	Services	Type	Bind services	Action	Log	Time
1	10.0.0.0/255.255.255.0	Aker - Spam Meter					
2	10.4.0.167	Aker - AV					

Image 404 – Profiles: VPN-SSL (Proxy SSL).

This tab allows configuring the services in order to get access to them through SSL Proxy or VPN SSL by users who fit in this access profile. Its format is the same as the ones in the filtering rules window with the exception that the source entities for the rule must not be specified and not all the options are available (for more information see the chapter **Stateful inspection**).

N.: Filtering rule number.

Destination: In this column the connection destination can be controlled.

Services: Indicates the protocol communication port.

Type: Indicates the SSL connection type, it may be direct or through applet.

The direct connection is denominated SSL Reverse Proxy, allowing the use of X.509 certificates with key size 1024, 2048 or 4096 bits. The client opens a SSL connection with the firewall, and the firewall opens a regular connection with the server.

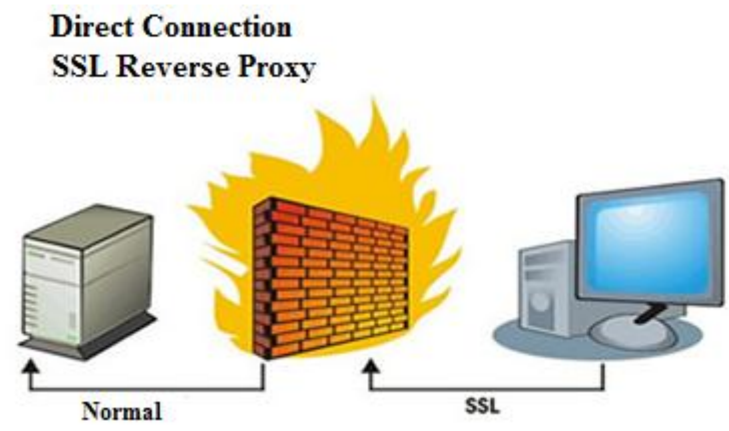

Direct Connection
SSL Reverse Proxy
Normal
SSL

Image 405 – Direct connection: SSL Reverse Proxy.

On the connection via applet, the client opens a connection via SSL with the firewall through a web page. The firewall provides a redirecting applet that the client will download to his machine. This applet starts a connection with the firewall via SSL, and the firewall starts a connection with the server.

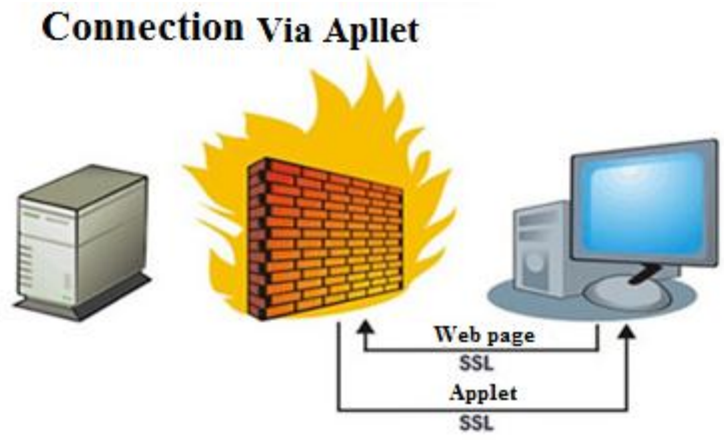

Connection Via Apllet
Web page
SSL
Applet
SSL

Image 406 – Connection via Apllet

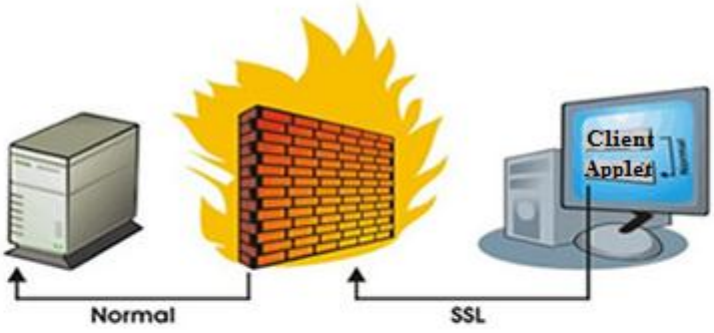


Image 407 – Connection Client Applet / SSL / Normal

Bind service: Indicates the communication port where the applet will start the service. For this one or more entities service type must to be added.

Action: This field defines what action will be taken for all packets that fit in this rule. It consists of two options, the description follows below:

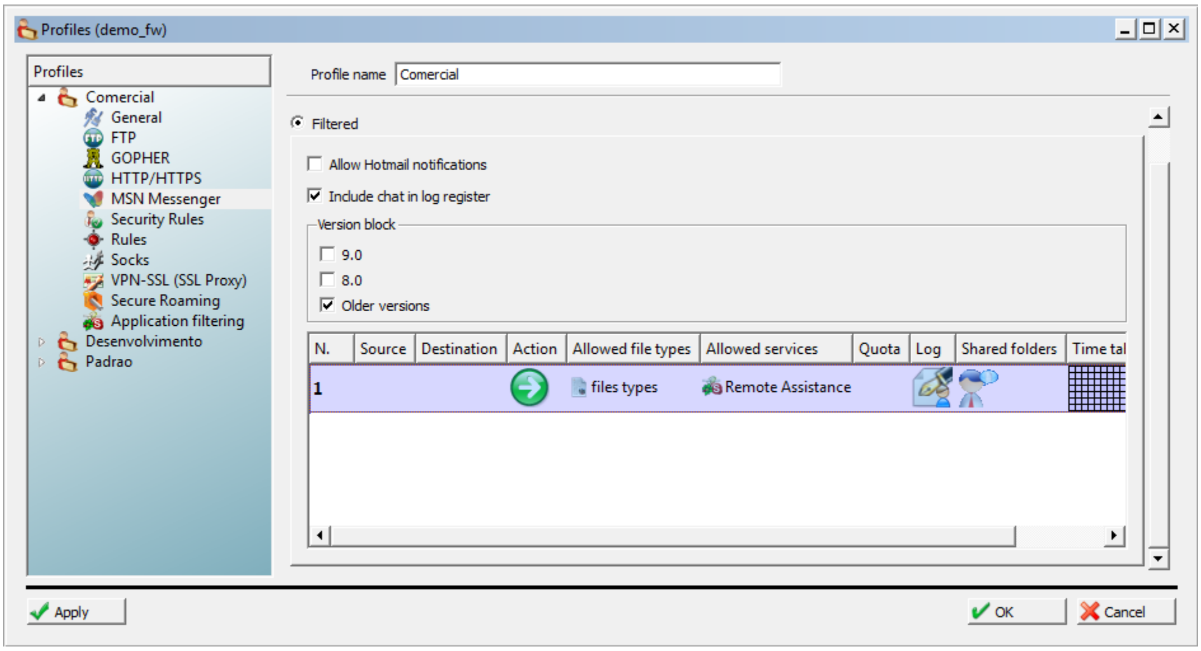
- **Accept:** Authorizes the packets that fit in the rule to pass through the firewall;
- **Reject:** This option does not allow the packets that fit in the rule to pass through the firewall. This way an ICMP packet will be sent to the packet source host informing that the destination is unreachable. This option does not work for some types of ICMP services due to a characteristic of this protocol.

Log: Defines what types of action will be performed by the system when the packet fits in the rule. It consists of several options that can be selected regardless one another.

TIme: Defines the time and weekday that the rule will be applied. The lines represent the weekdays and the columns represent the time.

The filtering rules for access profile consider as source the machine which the session was established. Due this, it is necessary specify just the destination entities and services that can be accessed.

23.10. MSN Messenger


Profiles (demo_fw)
Profiles
Comercial
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: Comercial

● Filtered

☐ Allow Hotmail notifications

☑ Include chat in log register

Version block

☐ 9.0

☐ 8.0

☑ Older versions

N.	Source	Destination	Action	Allowed file types	Allowed services	Quota	Log	Shared folders	Time tal
1				files types	Remote Assistance				

Image 408 – Profiles – MSN Messenger.

This tab configures the use of MSM Messenger and its services, for more information see the chapter **Configuring the MSN proxy**. The available options are:

Allow MSN Messenger: If this option is unchecked uses belonging to this profile will not be allowed to use The MSM Messenger, even if there is a filtering rule allowing this access.

It is crucial that the Messenger MIME type be blocked on the HTTP proxy; otherwise the access to Messenger will be possible through this service. This blocking option is already configured as default.

Unfiltered: This option is available only if the Allow MSM Messenger check box is marked, it indicates that the user can use the MSN Messenger, without any filtering.

Filtered: This option is available only if the Allow MSM Messenger check box is marked, it indicates that the user can use the MSM Messenger, but through a filtering rule.

Allow Hotmail notifications: This option is available only if the check box *Allow MSM Messenger* be marked; it allows the user to receive notifications of messages available on Hotmail.

Include chat in log register: This option records all chats among users.

Version Block: This option allows you to block the specific versions of MSN Messenger client.

In case you have selected the filtered access to MSM Messenger is necessary create one or more rules in order to define the type of access will be granted. In order to create any rule, right-click and the following image will be displayed:

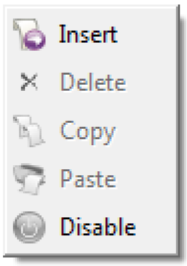


Image 409 – Option menu (Insert/disable) to perform any operation on the rule.

- **Insert:** Adds a new rule to the list.
- **Delete**: Deletes the selected rule from the list.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes the rule you have copied.
- **Disable:** Disables or enable the selected rule.

Each MSN rule consists of the following options:

Source: User e-mail address that has sent a message i.e. started the chat.

Destination: In this column you can control who the internal users will chat with. In order to do this, one or more entities e-mail types should be added (for more information see the chapter **Registering Entities**), containing the e-mail list or allowed domains.

Allowed files types: In this column you can set the file types that can be send/received through MSM Messenger. In order to do this one or more entities *file type list* should be added (for more information see the chapter **Registering Entities**) that contain the file type list allowed.

Allowed services: This column specifies which additional services can be used through *MSN Messenger*. The definition of services types is possible and done in the MSN proxy configuration. For more information see the chapter titled **Configuring the MSN proxy**.

Log: If this option is checked, information about the chats of all users will be registered. The following data will be available in the log: Logon/logoff of user, file transfer, use of additional service is the beginning and the end of chats.

Shared folders: In this option you can allow or not the users to share their folders on MSN.

Time table: Defines the time that the user will be allowed to user the MSM Messenger.

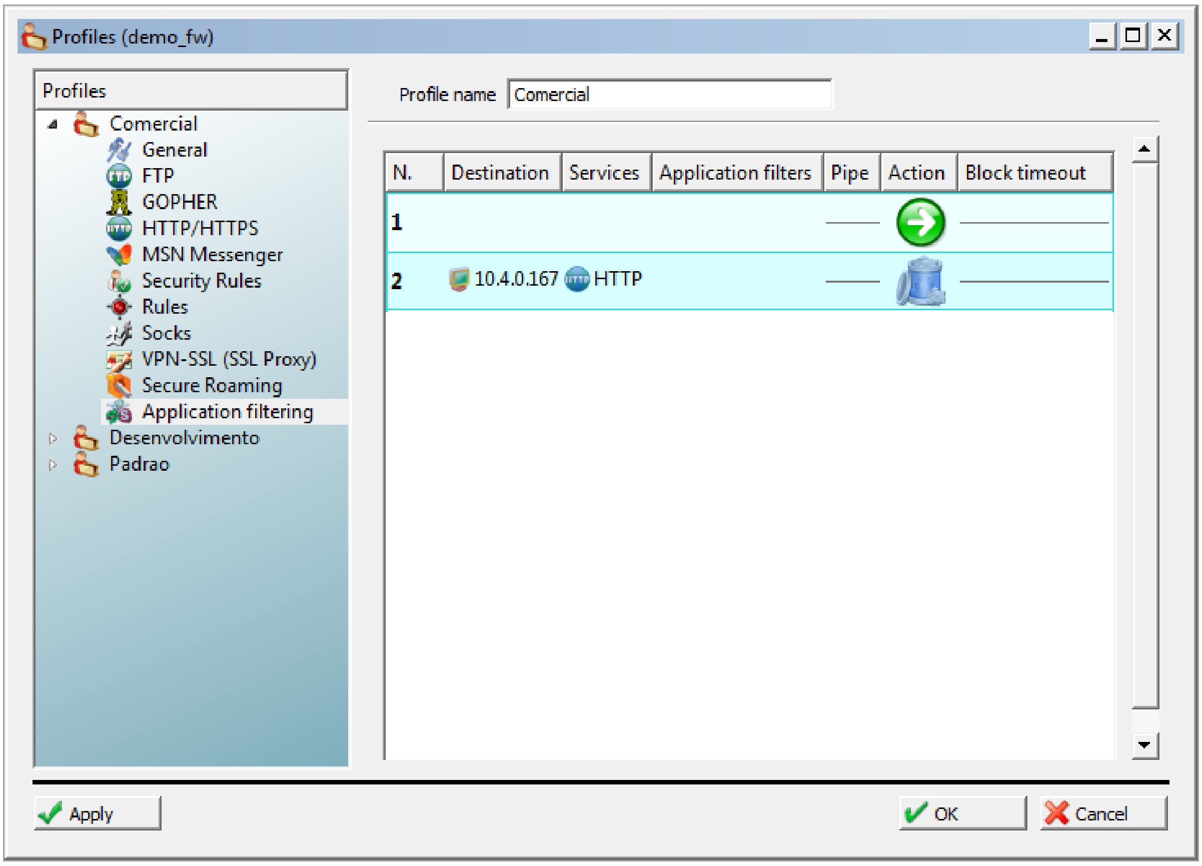
Action: Defines the action that will be executed in case the address that the user wants to access does not fit in any rule in the filtering rule. It consists in two options:

Allow: If this option is selected the firewall will accept the URLs that do not fit in any rule.

Block: If this option is selected the firewall will reject the URLs that do not fit in any rule.

Quota: Quotas are used to control and rationalize the time used by employees access the websites. This way the "Quotas" are the limits of the access time and the data volume.

23.11. Application filtering


Profiles (demo_fw)
Profiles
Comercial
General
FTP
GOPHER
HTTP/HTTPS
MSN Messenger
Security Rules
Rules
Socks
VPN-SSL (SSL Proxy)
Secure Roaming
Application filtering
Desenvolvimento
Padrao
Apply
OK
Cancel

Profile name: Comercial

N.	Destination	Services	Application filters	Pipe	Action	Block timeout
1				—	➔	—
2	10.4.0.167	HTTP		—		—

Image 410 – Profiles: Application filtering.

This tab allows configuring the rules to application filter. This rules allow specific types of files be blocked regardless of its extension or protocol which is being used to send them. It is possible instead of blocking just change a priority of a service or type of file which is being transferred.

The main importance of this filter is optimizing the Internet access. It is possible that all users have fast access to the Internet, but when they attempt to download files which are not considered important as mp3 songs, videos, etc., the connection which is being used to transfer theses files automatically will have its connection bandwidth reduced.

Bellow follows the available options:

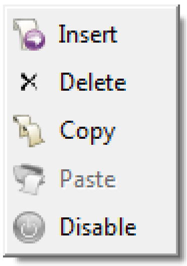


Image 411 – Option menu (insert/disable) to perform any change on the rule.

- **Insert:** Adds a new rule to the list.
- **Delete**: Deletes the selected rule from the list.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes the rule you have copied.
- **Disable:** Disables or enable the selected rule.

Each MSN rule consists of the following options**:**

Destination: Specifies the communication destination which the filter will be inspecting, in order to do this one or more entities machine types, network or sets should be added (for more information see the chapter titled **Registering entities**).

Services: Specifies the communication services that the filter will be inspecting, in order to do this one or more entities machine types, network or sets should be added (for more information see the chapter titled **Registering entities**).

Application filters: Indicates which filters will be active for the connections that go towards one of the destinations specified in the rule. The filter definition is made in the Application filters window. For more information see the chapter titled **Configuring the Application filters.**

Action: This column indicates the action that will be taken by the firewall in case one of the specified filters is applied. It consists of the following options:

Accept: Allows the connection to pass through the firewall.

Rejects: Does not allow the connection to pass through the firewall and send back a *reset packet* to the communication source machine.

Discard: The connection will not pass through the firewall, and now packet will be sent to the source machine.

Change priority: The connection will be accepted, but with a different priority that will be set in the **PIPE** column.

Block source: Indicates that the connection that has started the connection will be block for a while (it means all connection originated from it will be denied). The Block Timeout is used to specify the time that the machine will remain blocked.

Pipe: This column will be available only if the **Change priority** option is enabled. It indicates which new priority will be assigned to the connection. In order to do this, an entity pipe type should be added (for more information see the chapter titled **Registering entities**).

Block timeout: This column will be available only if the **Block source** is enabled. It indicates time that the source machine will remain blocked.

23.12. Associating users with access profile

Once the access profiles are created it is necessary associate them with users and groups of one or more authenticators or certified Authorities of the firewall.

To gain access to the authentication window follow the steps bellow:

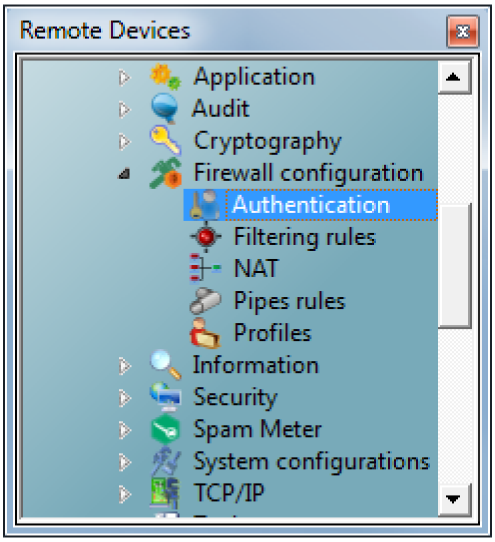
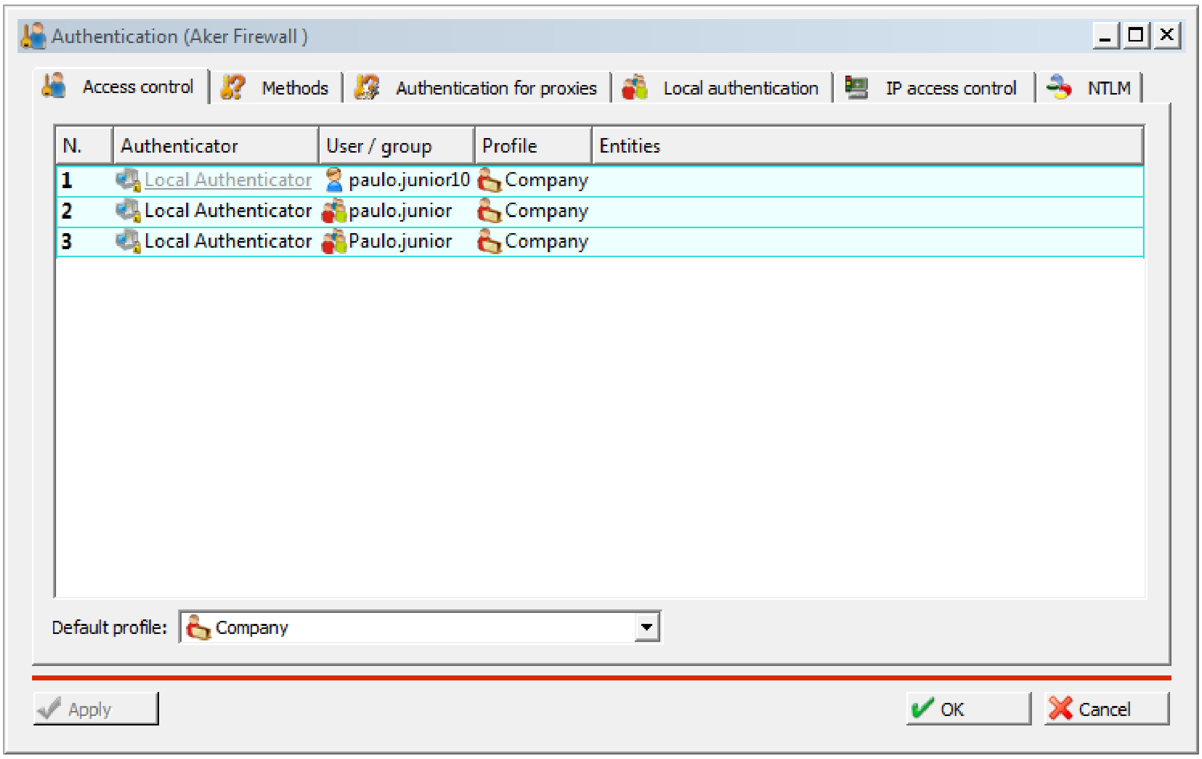

Remote Devices
Application
Audit
Cryptography
Firewall configuration
Authentication
Filtering rules
NAT
Pipes rules
Profiles
Information
Security
Spam Meter
System configurations
TCP/IP

Image 412 – Access window: Authentication.

- Click on the *firewall configuration* menu.
- Select *authentication*.
- Select the *access control* tab*.*

Access control tab


Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

N.	Authenticator	User / group	Profile	Entities
1	Local Authenticator	paulo.junior10	Company	
2	Local Authenticator	paulo.junior	Company	
3	Local Authenticator	Paulo.junior	Company	

Default profile: Company

Image 413 -Authentication: Access control.

The access control tab allows the users/groups association with the access profile.

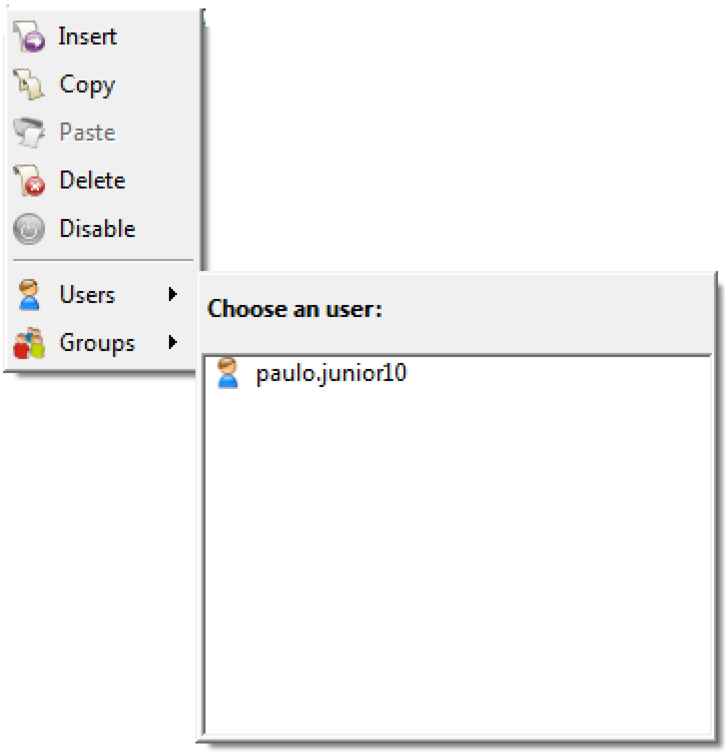
At the bottom of this window there is a field named **Default profile** where it is possible to select the profile which will be associated to users who do not fit in any association rule.

The last **Entities,** when filled it specifies networks and machines where the association is valid. If the user fits in the rule, but it is in an IP address that does not belong to registered networks or users, them the rule will be skipped, allowing the assignment of another profile to user:

To associate use or group to a specific access profile follow the steps bellow:

1. Right-click on the rules list and select the option **Insert.**
2. Select the authenticator which you want to get the users or group list from by right-clicking on the *Authenticator* field. For more information about authenticators, see the chapter titled **Configuring authentication parameters**.

3. Right-click on the *User/group* field and select between user and group list, the selected list will be mounted automatically through the selected authenticator. Through the list select the desired user and group.


Insert
Copy
Paste
Delete
Disable
Users
Groups
Choose an user:
paulo.junior10

4. Right-click on the Profile filed and choose the desired profile:

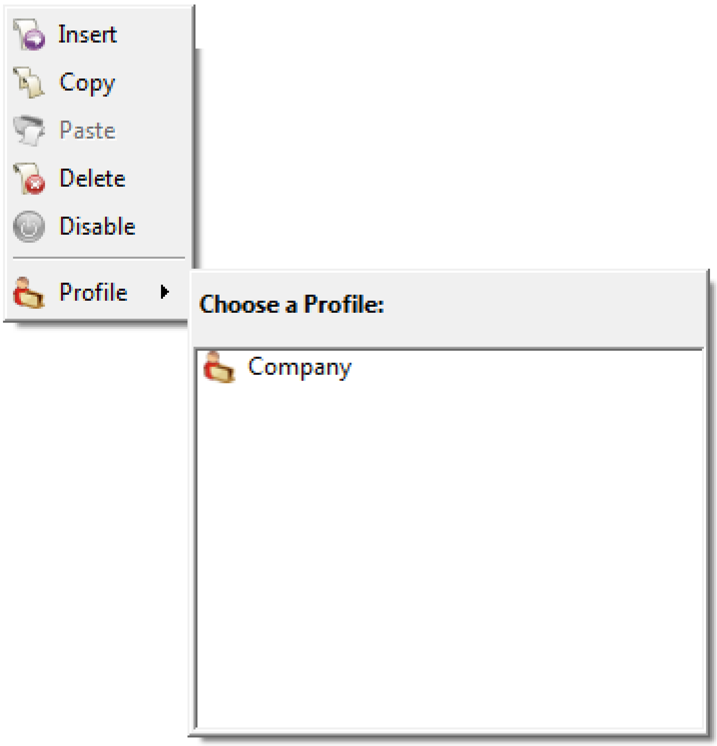


Image 415 – Choosing a new profile.

5. You also can drag one of the hosts, set or network entities to the entities field in the access control.

To remove a rule between a user/group and a profile, follow the steps bellow:

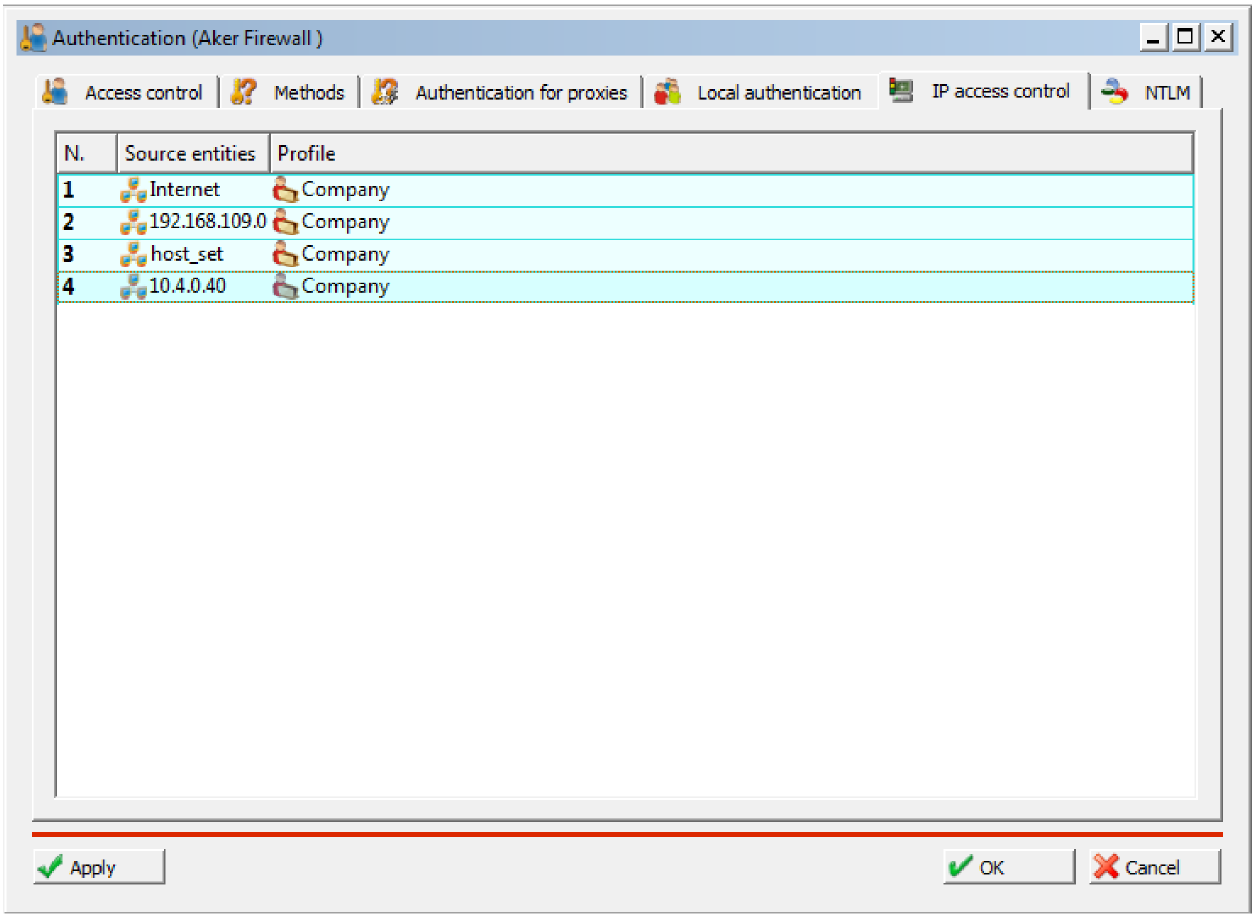
1. Click on the rule selected to be removed
2. Hit the **delete** key on your keyboard or right-click and select the **Delete** option.

To change a rule position in the list, follow the steps bellow:

1. Click on the rule you wish to move.
2. Drag it to the desired position.

The order of associations in the list is extremely important. When a user is authenticated, the firewall will search the list from the beginning looking for this user name or group that he belongs to. As soon as it is found the name or group, the profile assigned to it will be used.

IP access control tab



Authentication (Aker Firewall)
Access control
Methods
Authentication for proxies
Local authentication
IP access control
NTLM
Apply
OK
Cancel

N.	Source entities	Profile
1	Internet	Company
2	192.168.109.0	Company
3	host_set	Company
4	10.4.0.40	Company

Image 416 – Access control through IP.

The firewall can control the access through known IP addresses together with the profiles created to this end. In order to do this the administrator needs to register the known network, and drag it to the *Source entities* position, then add in the *Profile column* the profile necessary in this rule.

User authentication

24. User authentication

This chapter shows what is Aker Authentication Client and the usage of this appliance that provides a higher level of security.

24.1. Viewing and removing users connected to the Firewall

It is possible to view in any moment the users who have established connection with the firewall, through the authentication client, and remove one of these sessions. It is done in the ***Logged users*** window:

To gain access to the ***Logged users*** window, follow the steps below:

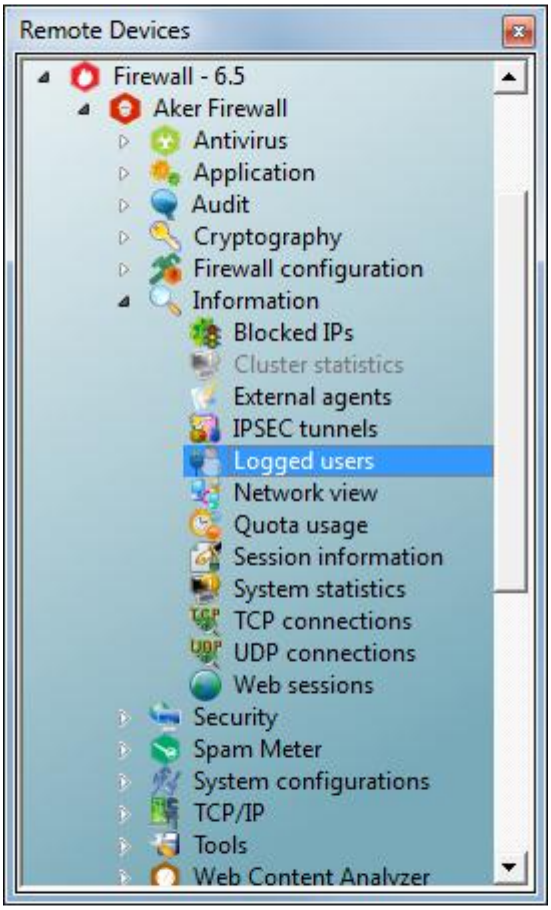
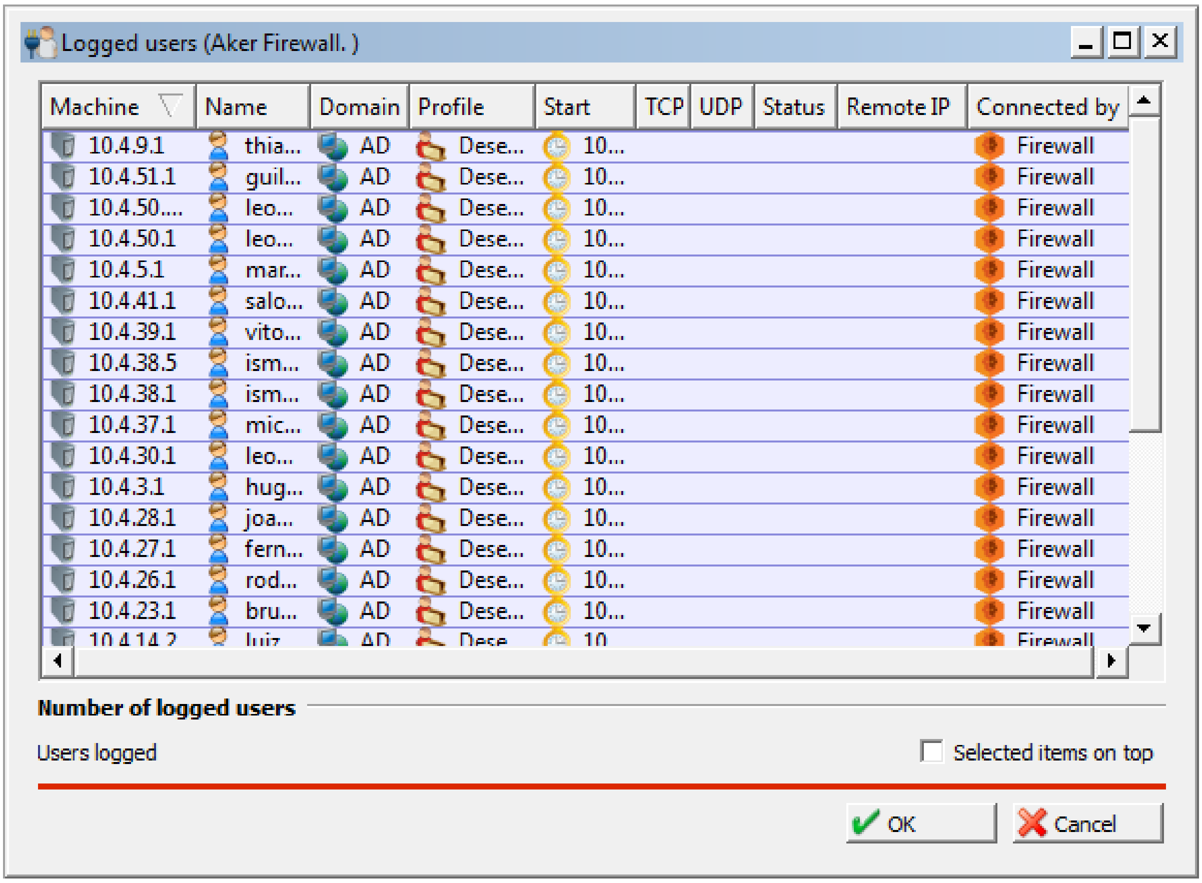

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 417 – Logged users.

- Click on the *Information* menu
- Select *Logged users*.

Logged users window



Logged users (Aker Firewall.)

Machine	Name	Domain	Profile	Start	TCP	UDP	Status	Remote IP	Connected by
10.4.9.1	thia...	AD	Dese...	10...					Firewall
10.4.51.1	guil...	AD	Dese...	10...					Firewall
10.4.50....	leo...	AD	Dese...	10...					Firewall
10.4.50.1	leo...	AD	Dese...	10...					Firewall
10.4.5.1	mar...	AD	Dese...	10...					Firewall
10.4.41.1	salo...	AD	Dese...	10...					Firewall
10.4.39.1	vito...	AD	Dese...	10...					Firewall
10.4.38.5	ism...	AD	Dese...	10...					Firewall
10.4.38.1	ism...	AD	Dese...	10...					Firewall
10.4.37.1	mic...	AD	Dese...	10...					Firewall
10.4.30.1	leo...	AD	Dese...	10...					Firewall
10.4.3.1	hug...	AD	Dese...	10...					Firewall
10.4.28.1	joa...	AD	Dese...	10...					Firewall
10.4.27.1	fern...	AD	Dese...	10...					Firewall
10.4.26.1	rod...	AD	Dese...	10...					Firewall
10.4.23.1	bru...	AD	Dese...	10...					Firewall
10.4.14.2	luiz	AD	Dese	10					Firewall

Number of logged users

Users logged

☐ Selected items on top

Image 418 – Connected users (host, name, domain, profile, start, TPC and the number of logged users.)

This window consists of a list with an entry for each user. At the bottom of this window there is a message showing the total amount of connected users. For users connected via Secure Roaming, the connection data (IP address and ports) will also be displayed.

- The ***Selected items on top*** option sets the items that have been selected to the top of the window.

Logged users toolbar:

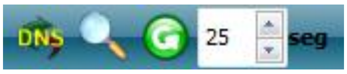


Image 419 – logged users toolbar.

- The **refresh button** updates the information periodically in an automatically way or not. The update interval can be set by changing the value next to the Refresh button.

- The **search button** allows removing a user’s session. In order to perform it, click on the session you wish to remove and click on the search button (if there is no session selected this option will be disabled)
- The **DNS button** will add the service names to resolve the host’s name whose IP addresses are listed. Below follows important points :

  1. The name resolution often is slow, and due to it the name translation is done in background.
  2. Often due to the reverse DNS configuration problems (which is used to resolve names through IP address), the resolution of certain addresses will not be possible. In this case the addresses not resolved will be maintained in the original form and will be indicated that they do not have a reverse DNS configured.

Meaning of an active user session

Each line existing in the user session list represent a session. The meaning of its field is displayed below:

Icon: It is displayed on the left of each user name and it can take three distinct forms:

Lock: This icon indicates that the user has been logged only through encryption client.

User: This icon indicates that the user has been logged only through authentication client.

User in the lock: This icon indicates that the user has been logged only through encryption and authentication client.

Machine: Machine IP address or name (in case the DNS is active) which the session has been established.

Name: User name who has established the session.

Domain: Domain name, i.e. authenticator, which the user has been authenticated. In case user does not have a specific domain when logging, this field will be displayed in black.

Profile: Access profile corresponding to this session, if this field is in blank, user has been authenticated before the profile table be changed, so it is using a profile that no long exist.

Start: Time and date that the session started.

24.2. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action).*

Program location*: /aker/bin/firewall/fwlist*

Syntax:

```
fwlist – Lists and removes TCP/UDP connections and  active sessions

Usage: fwlist help

    fwlist show [[-w] [TCP | TCP6]] | [UDP | UDP6]

    fwlist show [sessions | roaming | blocked]

    fwlist show [quotas | www]

    fwlist remove [TCP | TCP6 | UDP | UDP6] source_IP source_Port

                destination_IP destination_Port

    fwlist remove sessions source_IP [user]

    fwlist remove blocked source_IP

    fwlist restart [ user <name> ] [ quota <name> ] [time] [volume]


    help    = shows this message

    show   = lists active connections or sessions

    remove   = removes an active connection or session

    restart = restarts users quota
```

Example 1: (listing the logged user session in the firewall)

```
#fwlist show session

Name/Domain Profile source IP start
------------------------------------------------------------------------------
administrator/BSB Admin 10.20.1.1 08:11:27
jose.silva/GOA Default5 10.45.1.1 07:39:54
```

```
joao.souza/POA Default3 10.57.1.1 07:58:10
josemaria/GRU Default3 10.78.1.1 08:01:02
angelam/BSB 1 Restricted 10.22.1.1 08:48:31
marciam/POA Restricted 10.235.1.1 10:49:44
antonioj/POA Especial 10.42.2.1 06:02:19
operador/BSB Default 10.151.2.1 20:44:34
```

Example 2: (removing the logged user session from machine 10.19.1.1)

```
#fwlist remove session 10.19.1.1


The session removal has been selected by the user server.
```

Configuring the SMTP proxy

25. Configuring the SMTP proxy

This chapter shows which are the functions offered by SMTP proxy and how to perform its configuration.

What is SMTP proxy?

The SMTP proxy is a specialized program of Aker Firewall, designed to work with electronic mail (SMTP is an anagram for *Simple Mail Transfer Protocol,* the full name of electronic mail transfer service on the Internet). This proxy enables the filtering of e-mail messages based on their contents or on any field of their header. It also works as a barrier protecting the SMTP server against several types of attacks.

It is a transparent proxy (for more information see the chapter titled Working with proxies), thus, neither the server nor the client knows about its existence.

Description of a SMTP message

In order to understand the fields filtering of the SMTP proxy, some information about the e-mail messages are necessary.

An e-mail message is formed by three distinct parts: envelop, header, and body. Each of these parts has specific information.

- **Envelop**

  Envelop is called this way because it is similar to envelop of a standard letter. It contains basically the sender and the recipients of a message. For each recipient of a different domain, a new envelop is generated. This way, a SMTP server receives in envelop of a message the name of all recipients of the message which are part of its domain.

  Envelop is not seen by the recipients of a message. It is used only between SMTP servers.

- **Header**

  The message header contains several pieces of information about the message, like the subject, date and sender's name. The header is usually displayed to the message recipient.

- **Body**

  The body contains the message, as it was generated by the sender.

Attacks against a SMTP server

There are several attacks which can be target against a SMTP server. They are:

- **Bugs exploits**

  In this case, the attacker tries to issue a command or arguments of a command that are known to generate security breaches.

  Aker Firewall SMTP proxy blocks these attacks allowing only the use of commands considered secure and validating the arguments of every command.

- **Buffer overflows**

  These attacks consist of generating large command strings, causing the servers that are not correctly developed to generate security failures.

  Aker Firewall SMTP proxy blocks these attacks limiting the maximum command strings that can be sent to the server.

- **Relay attacks**

  These attacks consist of using the SMTP server of another organization to send e-mail messages. This way, the computer resources that should be available for valid requests are consumed.

  Aker Firewall SMTP proxy, if correctly configured, blocks relay attacks.

Using the SMTP proxy

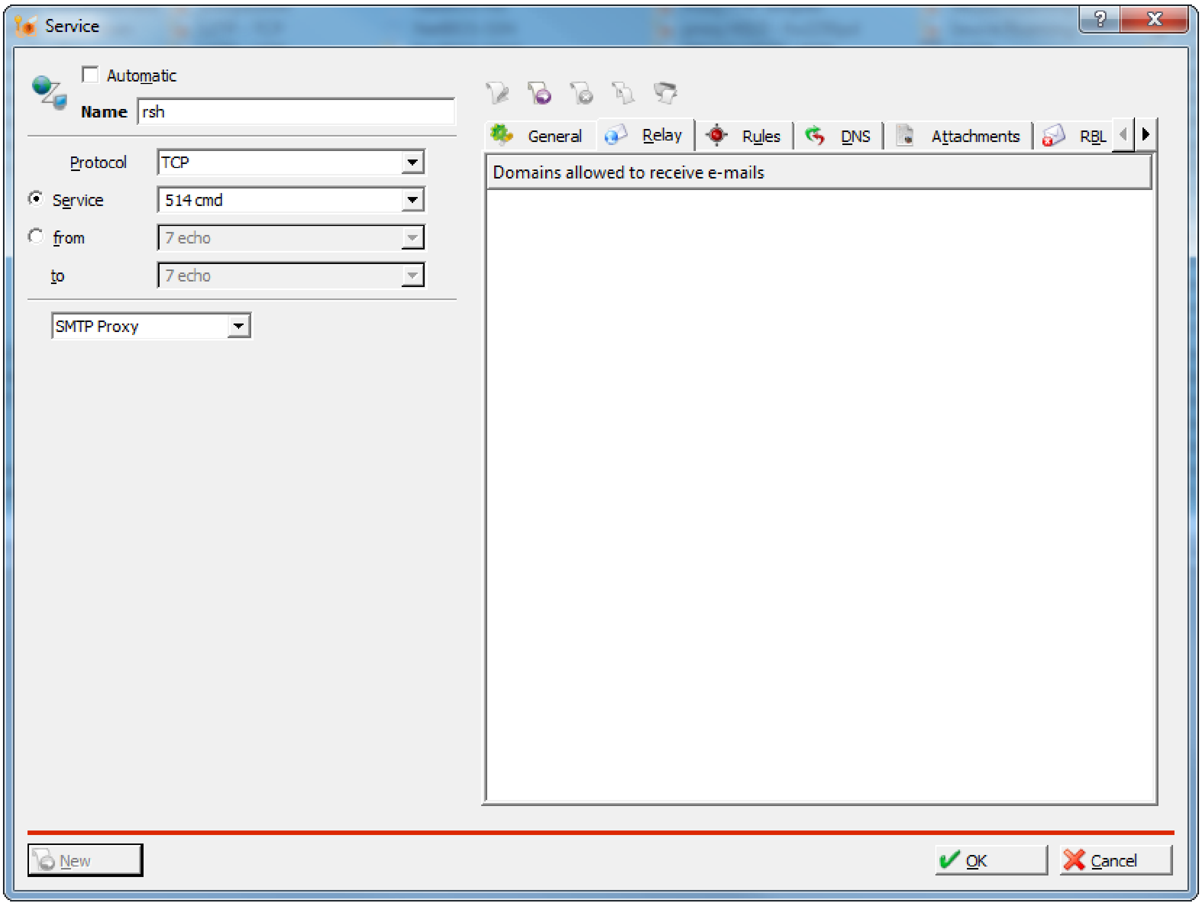
To use the SMTP proxy in a communication, it is necessary to follow two steps:

1. Create a service which will be redirected to the SMTP proxy and edit the parameters of the context to be used for this service (for more information, see the chapter titled **Registering Entities**)
2. Add a filtering rule allowing the use of the service created in the step 1, for the desired networks or hosts (for more information see the chapter titled **The Stateful Filter)**

25.1. Editing parameters of an SMTP context

The properties window of a SMTP context is displayed when the **SMTP proxy** option is selected, in the services edition window. Through this window it is possible to define the behavior of the SMTP proxy when dealing with a specific service.

The properties window of a SMTP context



☐ Automatic

Name: rsh

Protocol: TCP

● Service: 514 cmd

○ from: 7 echo

to: 7 echo

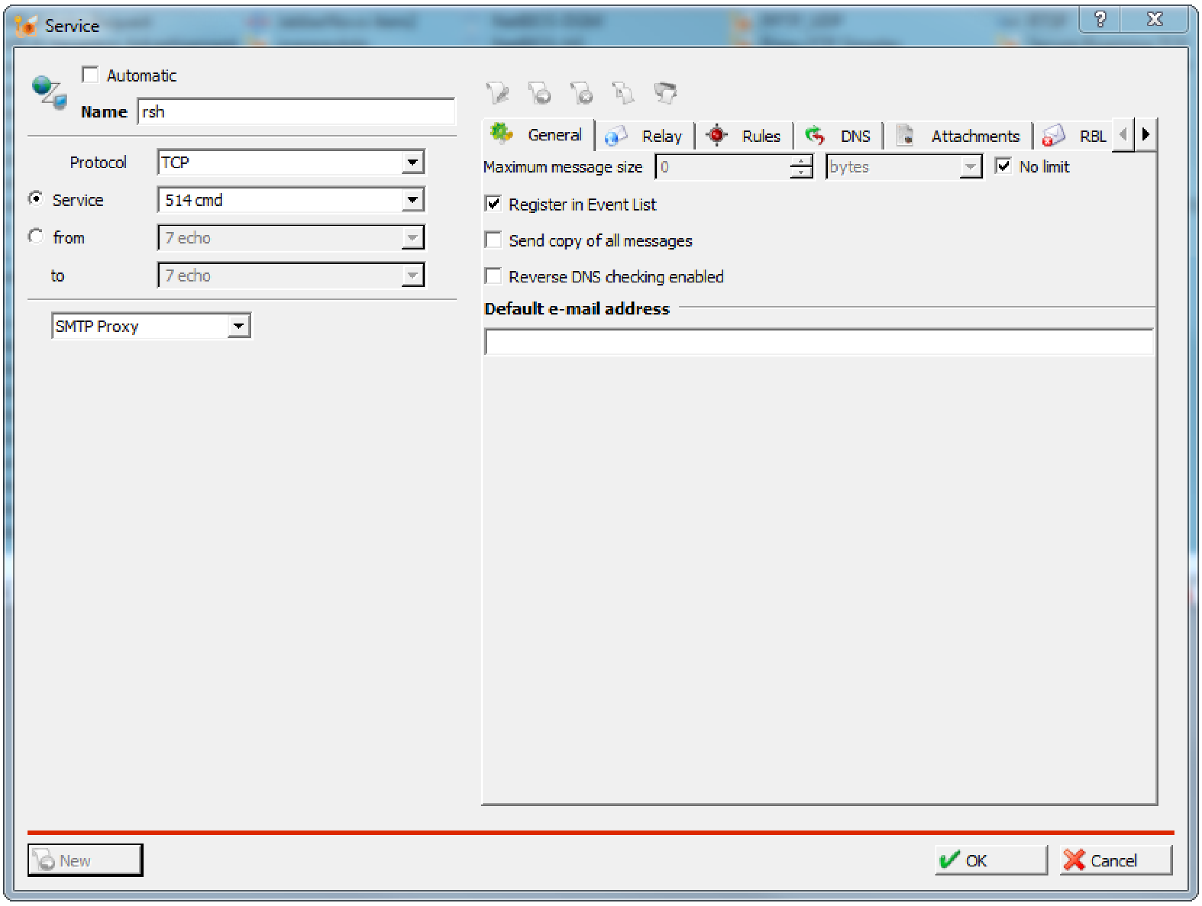
SMTP Proxy

Domains allowed to receive e-mails

Image 420 – Service: relay.

The properties window is where all parameters of a context, associated to a specific service, are configured.

General tab



☐ Automatic

Name rsh

Protocol TCP

● Service 514 cmd

○ from 7 echo

to 7 echo

SMTP Proxy

Maximum message size 0 bytes ☑ No limit

☑ Register in Event List

☐ Send copy of all messages

☐ Reverse DNS checking enabled

Default e-mail address

Image 421 – Service: general.

Maximum message size: This field indicates the maximum size (in bytes) of a message in order for it to be accepted by the proxy. If it is not desired to define a maximum size, it is only necessary to check the **No limit** option, located at the right of this field.

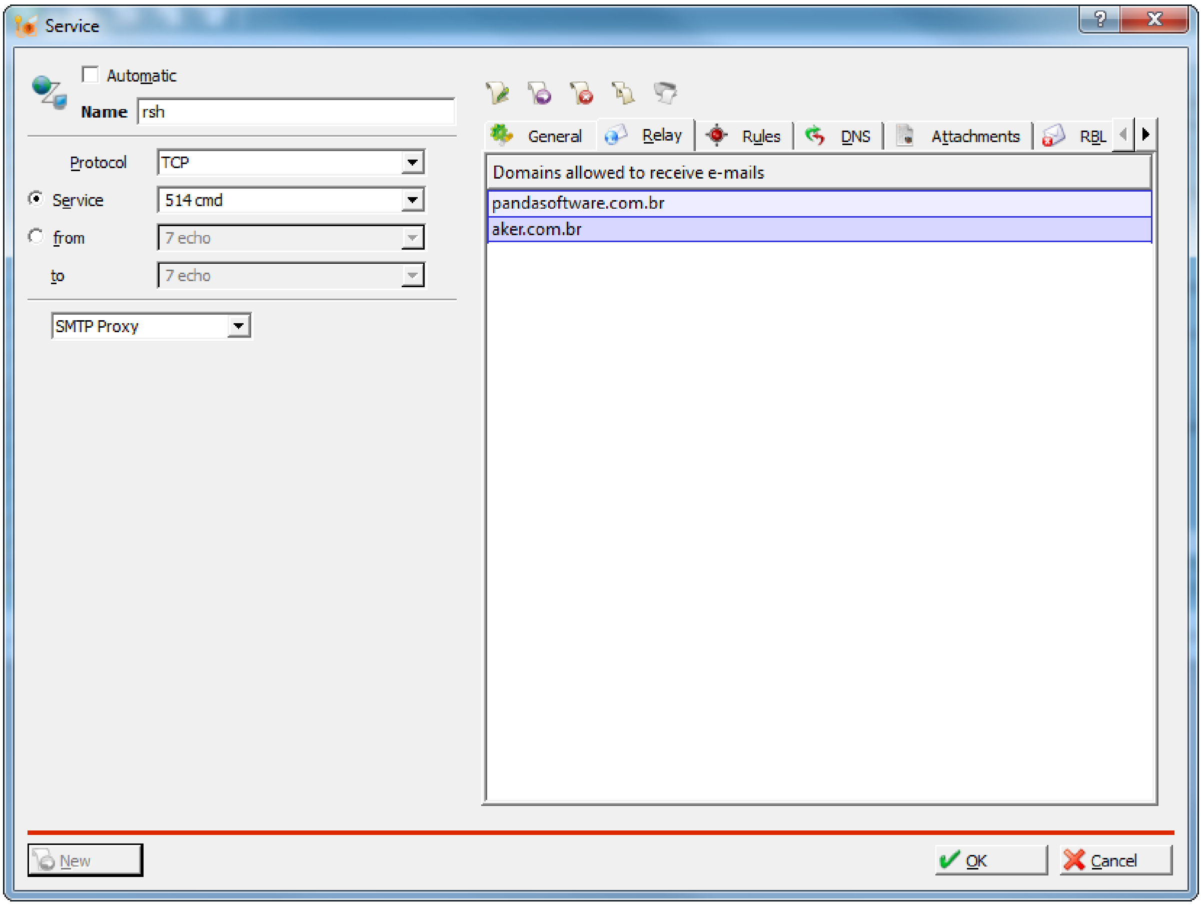
Register in the event list: This field indicates if the messages that do not match any SMTP rule of this context will be registered in the events list.

Send copy of all messages: Regardless of a message being accepted or rejected, it is possible to send a complete copy of the messages to any e-mail address. This field indicates if this copy will be sent or not.

Reverse DNS checking enabled: If this option is checked, only connections from hosts with a configured reverse DNS, pointing to a valid name, will be accepted.

Default e-mail address: It indicates the default e-mail address which the copies of messages that do not match any SMTP rule of this context will be sent to (if the option *Send copy of all messages* is checked). This e-mail can also be referenced in any filtering rule of the context.

Relay tab



☐ Automatic

Name: rsh

Protocol: TCP

● Service: 514 cmd

○ from: 7 echo

to: 7 echo

SMTP Proxy

Domains allowed to receive e-mails
pandasoftware.com.br
aker.com.br

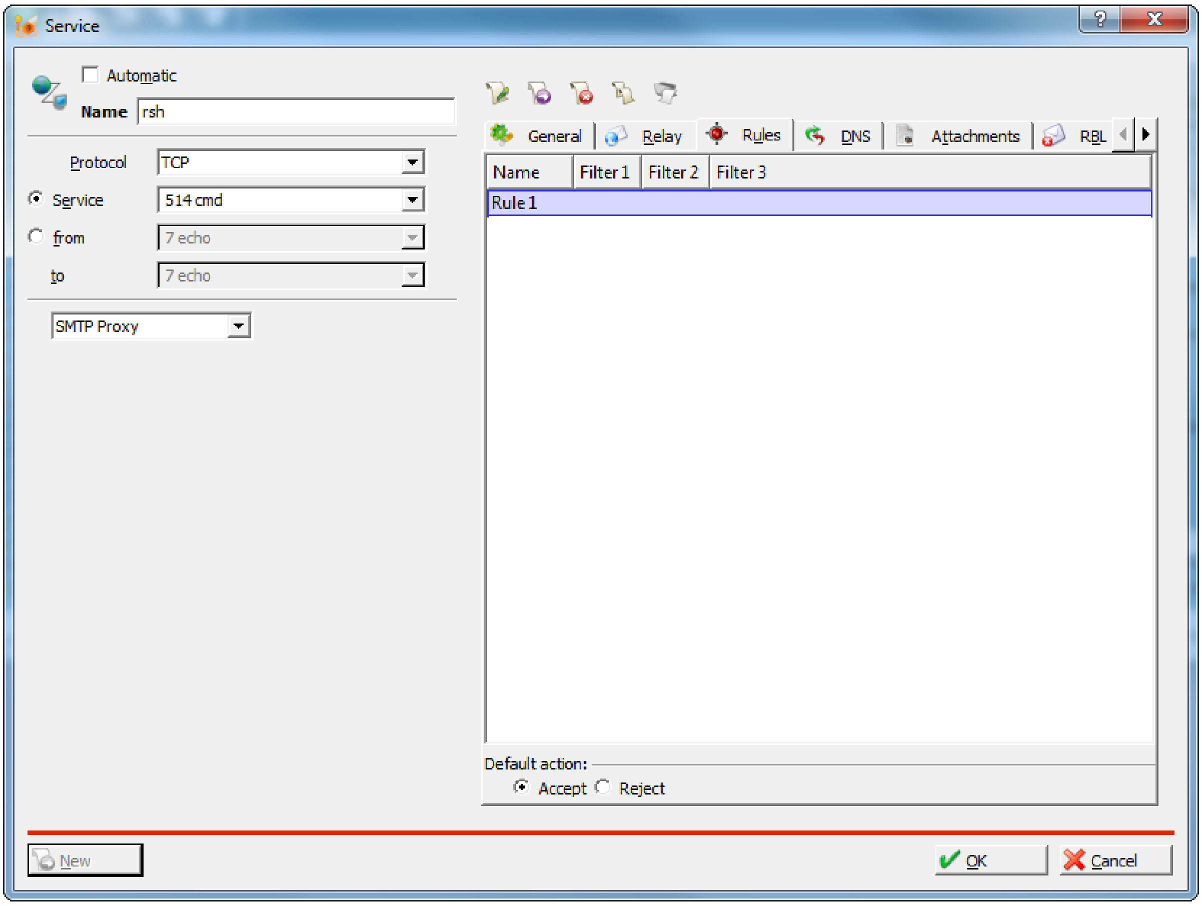
Image 422 – Service: relay.

This tab allows the administrator to specify a list of valid domains to receive e-mails. E-mails sent to any domain not listed will be rejected even before their transmission begins.

If the domain list is left blank the firewall will not protect against relay, i.e., it will accept e-mails destined to any domain.

Differently from the relay control provided by SMTP servers, the firewall can only base its control on the recipients of an e-mail, and not on the sender, since it does not have the list of valid users in the protected SMTP server.

Rules tab



☐ Automatic
Name rsh
Protocol TCP
● Service 514 cmd
○ from 7 echo
to 7 echo
SMTP Proxy

Name	Filter 1	Filter 2	Filter 3
Rule 1			

Default action: ● Accept ○ Reject

Image 423 – Service: rule.

In this tab all filtering rules for the context will be displayed. These rules allow the administrator to configure filters for e-mail messages based on their contents.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will be displayed: (this menu will be displayed whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).

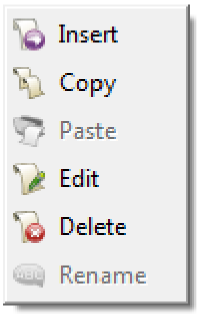


Image 424 – Option menu.

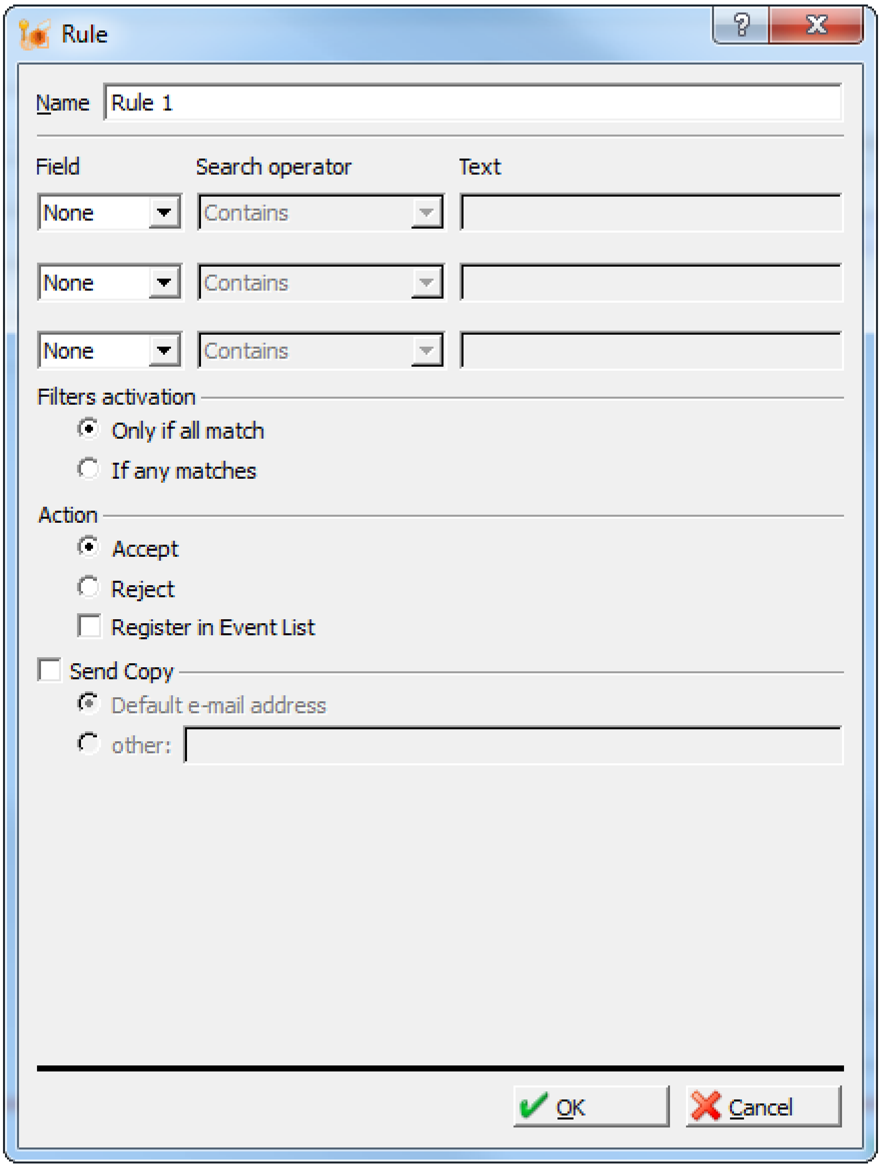
- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Edit:** This option opens the edition window for the selected rule.
- **Delete:** This option removes the selected rule from the list.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.
- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

  Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, clicking on it with the left button, and then click on the desired option.

The order of rules in the list is very important. Whenever the firewall receives a message, it will search the list from the beginning looking for a rule the message matches. As soon as it is found, the action associated to it will be taken.

In the case of insertion or edition of rules, the edit window, described in the section below, will be displayed:

SMTP rules edition


Rule

Name: Rule 1

Field	Search operator	Text
None	Contains	
None	Contains	
None	Contains	

Filters activation
● Only if all match
○ If any matches

Action
● Accept
○ Reject
☐ Register in Event List

☐ Send Copy
● Default e-mail address
○ other:

Image 425 – rule edition: SMTP.

All the parameters related to a filtering rule for a SMTP context are configured in this window. Each rule consists basically of 3 independent conditions that may or may not be filled (in other words, it is possible to create rules with only one or two conditions).

To create a rule, it is necessary to fill in the following fields:

Name: Name that identifies the rule in the context. This name will be displayed in the list of rules of the SMTP context. There cannot be two rules with the same name.

Field: Defines the name of the field within the SMTP message where the search will take place. It can take one of the following values:

- **NONE:** No search will be performed.
- **TO (All):** The search is performed in the destination address of the message (all of them must match the rule).
- **TO (Any)**: The search is performed in the destination address of the message (at least one has to match the rule).
- **FROM:** The search is done in the source address of the message.
- **CC:** The search is done in the list of address which will receive a copy of the message.
- **REPLY:** The search is done in the REPLY-TO field, indicating the address for which the message should be answered.
- **SUBJECT:** The search is done in the field that defines the subject of the message.
- **Header:** The search is done in all the fields that compose the header of the message.
- **Body**: The search is done in the body of the message (where the message effectively exists).

The TO and CC fields are treated differently by the SMTP proxy: the TO field is treated as a list of all message recipients, obtained from the message envelop. The CC field is treated as a simple text, obtained from the message header, and its usefulness is very limited.

Search: Type of search to be performed in the field defined above:

- **CONTAINS**: The field to be searched must contain the supplied text in any position.
- **DOESN'T CONTAIN**: The field to be searched must not contain the supplied text.
- **IS**: The content of the field to be searched must be exactly equal to the supplied text.
- **IS NOT**: The content of the field to be searched must be different of the supplied text.
- **STARTS WITH**: The content of the field to be searched must start with the supplied text.
- **DOESN'T START WITH**: The content of the field to be searched must not start with the supplied text.
- **ENDS WITH**: The content of the field to be searched must end with the supplied text.
- **DOESN'T END WITH**: The content of the field to be searched must not end with the supplied text.
- **CONTAINS WORDS**: In this type of search, the supplied text is considered as formed by individual words (separated by spaces), instead of a continuous text. To match the search, the field must contain all the given words, regardless of their positions.

Text: Text to be searched. This field is treated as a continuous text which will be compared with the specified field, except in case of the CONTAIN WORDS search, when it is treated as several words separated by spaces. **In both cases, this field is case-insensitive.**

The fields **Field, Search** and **Text** appear 3 times. Therefore, it is possible to define up to 3 different conditions that a message needs to fulfill in order to match the rule. If it is not desired to specify 3 conditions, just leave the value NONE on the parameter field of the conditions that will not be specified.

Filters activation: This option only makes sense when more than one condition is specified. It indicates what type of operation will be used to relate them.

- **Only if all match;** In order for a message to match the rule, it is necessary that it satisfy all conditions.
- **If any matches;** In order for a message to match the rule, it is necessary that it satisfy one of the conditions.

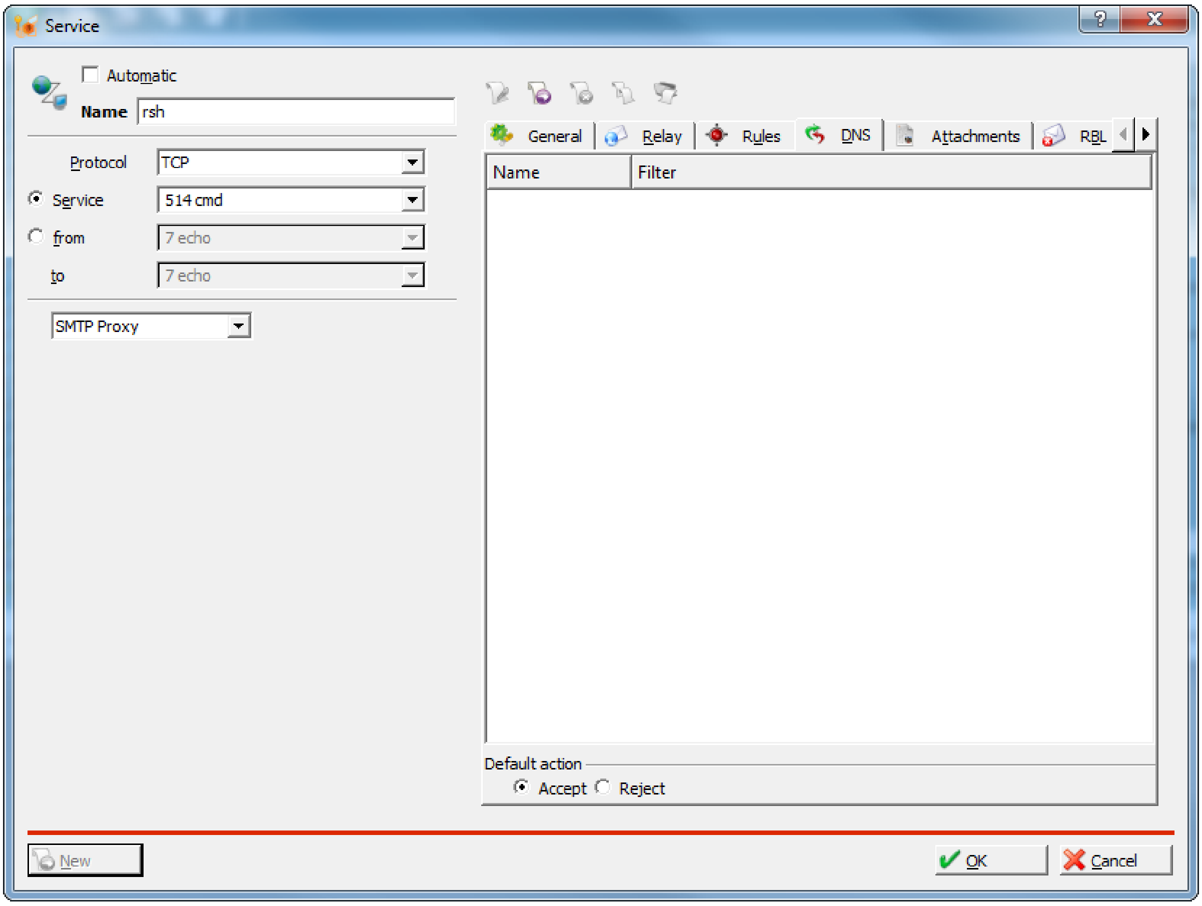
Action: The field indicates if the messages that match the rule should be accepted or rejected by the SMTP proxy.

Register in the event list: This field indicates if the messages that match the rule will be registered or not in the events list.

Send copy: For all messages that match the rule, regardless of being accepted or rejected, it is possible to send a complete copy of the message to any e-mail address. This field indicates if this copy will be sent or not. If it is checked, one of the following sending options must be chosen:

- **Default e-mail address:** The copy of the message will be sent to the default e-mail address.
- **Other:** The copy of the message will sent to the address specified in the field at the right.

DNS tab



☐ Automatic

Name rsh

Protocol TCP

● Service 514 cmd

○ from 7 echo

to 7 echo

SMTP Proxy

Default action

● Accept ○ Reject

Image 426 – Service: DNS.

In this tab all DNS filtering rules for the context will be displayed. These rules allow the administrator to configure e-mail filters based on the name returned by the reverse DNS of the SMTP server that will be sending the messages.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will be displayed: (this menu will be displayed whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).

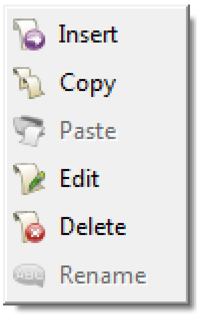


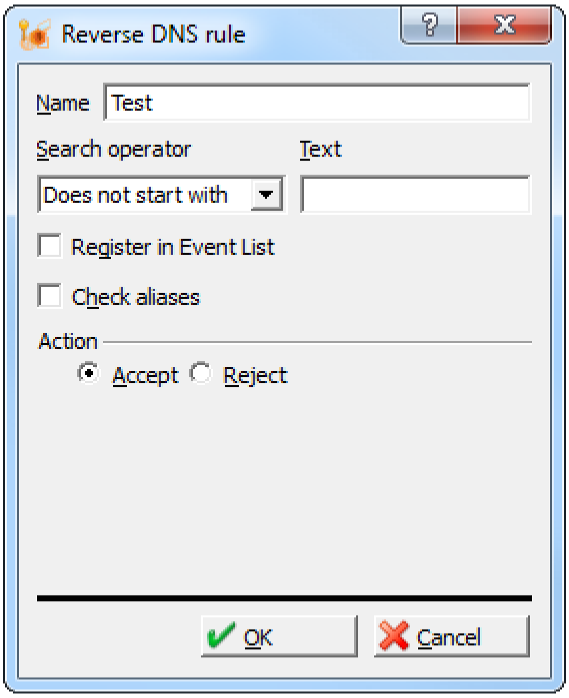
Image 427 – Option menu

- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Edit:** This option opens the edition window for the selected rule.
- **Delete:** This option removes the selected rule from the list.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.
- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, and then left-click on it, and select the desired option.

In the case of insertion or edition of rules, the edit window, described in the section below, will be displayed:

Reverse DNS rule



Name: Test

Search operator: Does not start with

Text:

☐ Register in Event List

☐ Check aliases

Action

● Accept ○ Reject

Image 428 – Service: DNS.

To create a rule, it is necessary to fill in the following fields:

Name: Name that identifies the rule in the context. This name will be displayed in the list of DNS rules of the SMTP context. There cannot be two rules with the same name.

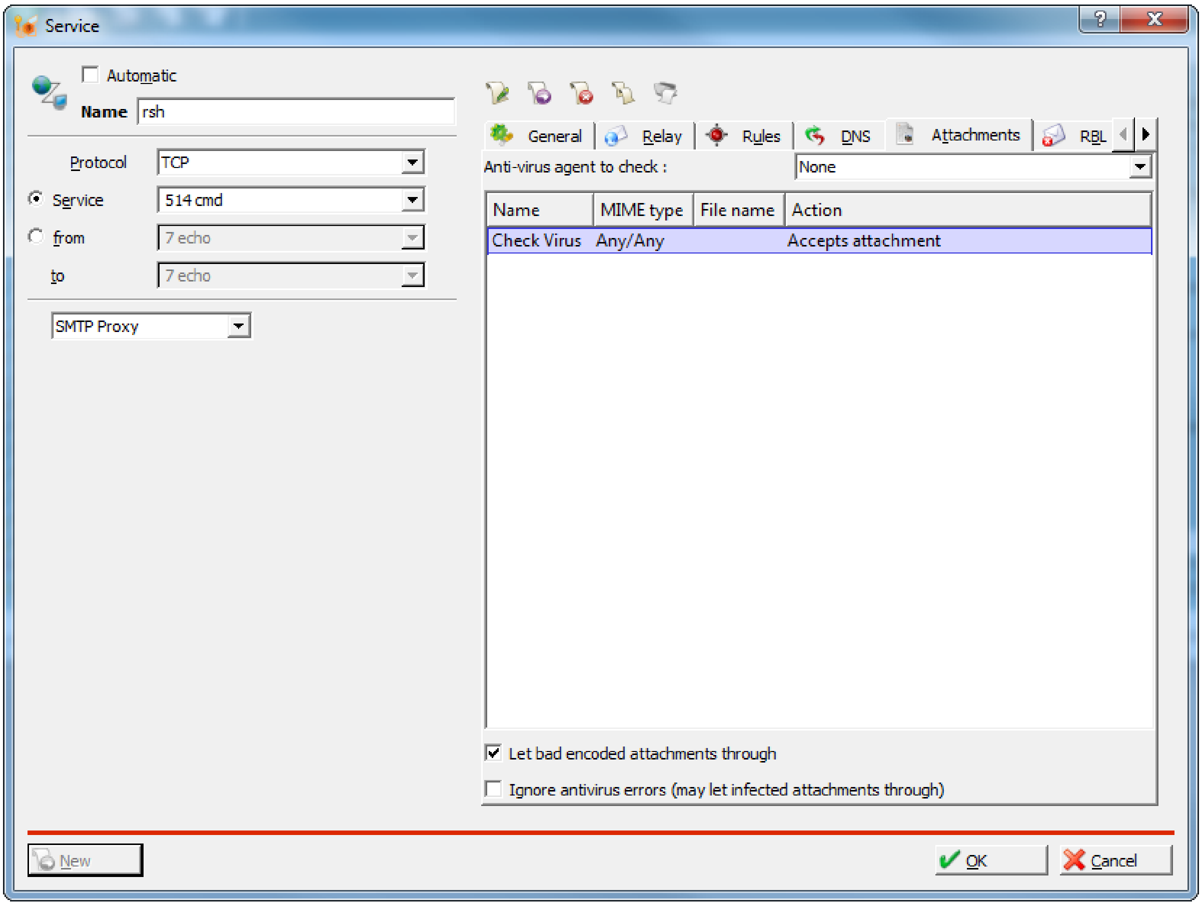
Search operator: The same operators used in the SMTP filtering rules can be used for reverse DNS filtering.

Text: Defines the text to be searched.

Check aliases: If this option is set, the firewall will compare all aliases returned by the DNS to see if any of them matches the rule.

Action: The field indicates if the messages that match the rule should be accepted or rejected by the SMTP proxy.

Attachments tab



☐ Automatic

Name: rsh

Protocol: TCP

● Service: 514 cmd

○ from: 7 echo

to: 7 echo

SMTP Proxy

Anti-virus agent to check : None

Name	MIME type	File name	Action
Check Virus	Any/Any		Accepts attachment

☑ Let bad encoded attachments through

☐ Ignore antivirus errors (may let infected attachments through)

Image 429 – Service: attachments.

This tab is used to specify rules to deal with attachments. These rules allow that, if a message was accepted, its attachments to be removed or scanned for viruses. They also permit that a fully message be rejected if it contains an unacceptable file (with virus, for instance).

Antivirus agent to check: This field specifies the antivirus agent that will be used to scan files attached to e-mails. This agent must have been previously registered in the firewall. For more information, refer to chapter **Registering entities**.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will be displayed: (this menu will be displayed whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).

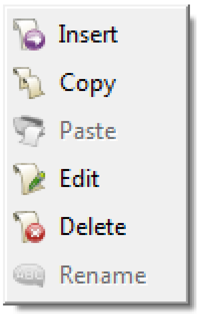


Image 430 – Option menu

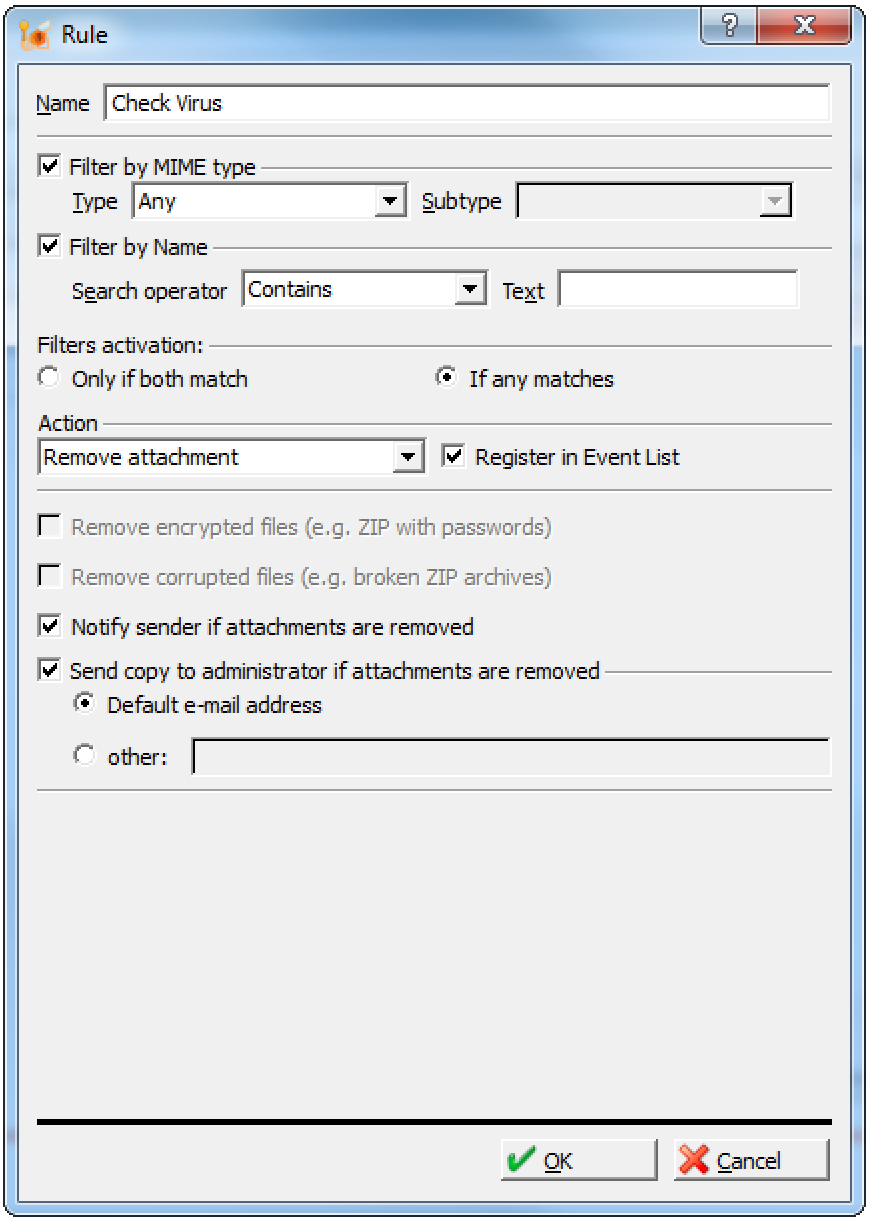
- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Delete:** This option removes the selected rule from the list.
- **Edit:** This option opens the edition window for the selected rule.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.
- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, clicking on it with the left button, and then click on the desired option.

The order of rules in the list is very important. For each attachment in a message, the firewall will search the list from the beginning looking for a rule that is matched. As soon as it is found, the action associated to it will be taken.

In the case of addition or edition of rules, the edit window, described in the section below, will be displayed:

Attachments rules edition



Name: Check Virus

☑ Filter by MIME type

Type: Any — Subtype:

☑ Filter by Name

Search operator: Contains — Text:

Filters activation:

○ Only if both match ● If any matches

Action: Remove attachment — ☑ Register in Event List

☐ Remove encrypted files (e.g. ZIP with passwords)

☐ Remove corrupted files (e.g. broken ZIP archives)

☑ Notify sender if attachments are removed

☑ Send copy to administrator if attachments are removed

● Default e-mail address

○ other:

Image 431 – Rule: edition of rules and attachments.

All the parameters related to a filtering rule for attachments for a SMTP context are configured in this window. It consists of the following fields:

Name: Name that identifies the rule in the context. This name will be displayed in the list of rules for attachments of the SMTP context. There cannot be two rules with the same name.

Filter by MIME type: This field allows the creation of an attachment filtering rule based on the MIME type of the attached file. When it is checked, it is necessary to specify its type and subtype.

Filter by name: This field allows the creation of an attachment filtering rule based on (part of) the name of the attached file. When it is checked, it is necessary to specify the type of search to be performed and the text to be searched. These fields are equal to the fields of the same name of the SMTP filtering rule, described above.

Search operator: This field is equal to the field of the same name of a SMTP filtering rule, described above.

Action: Indicates which action will be taken by the firewall when a file matches the rule. It consists of three options:

- **Accept attachment**: If this option is selected the firewall will keep the attached file in the message.
- **Remove attachment**: If this option is selected the firewall will remove the attached file from the message.
- **Discard message**: If this option is selected, the firewall will reject the message.
- **Remove infected attachment**: If this option is selected the firewall will scan the attached file. If a virus is found the firewall will take one of the following actions: if the file can be disinfected, the virus will be removed and the file re-attached to the message. If the disinfection is not possible, the firewall will remove the file and add a message informing the recipient of this fact.
- **Discard infected message**: If this option is selected the firewall will scan the attached file. If a virus is found the firewall will take one of the following actions: if the file can be disinfected, the virus will be removed and the file re-attached to the message. If the disinfection is not possible, the firewall will reject the message.

It is recommended the use of the actions that remove the attached files for incoming e-mails and the actions that reject the whole message in outgoing e-mails.

Remove encrypted files: If this option is checked, the firewall will remove the attachments that are encrypted and thus cannot be scanned.

Remove corrupt files: If this option is checked, the firewall will remove the attachments that are corrupted.

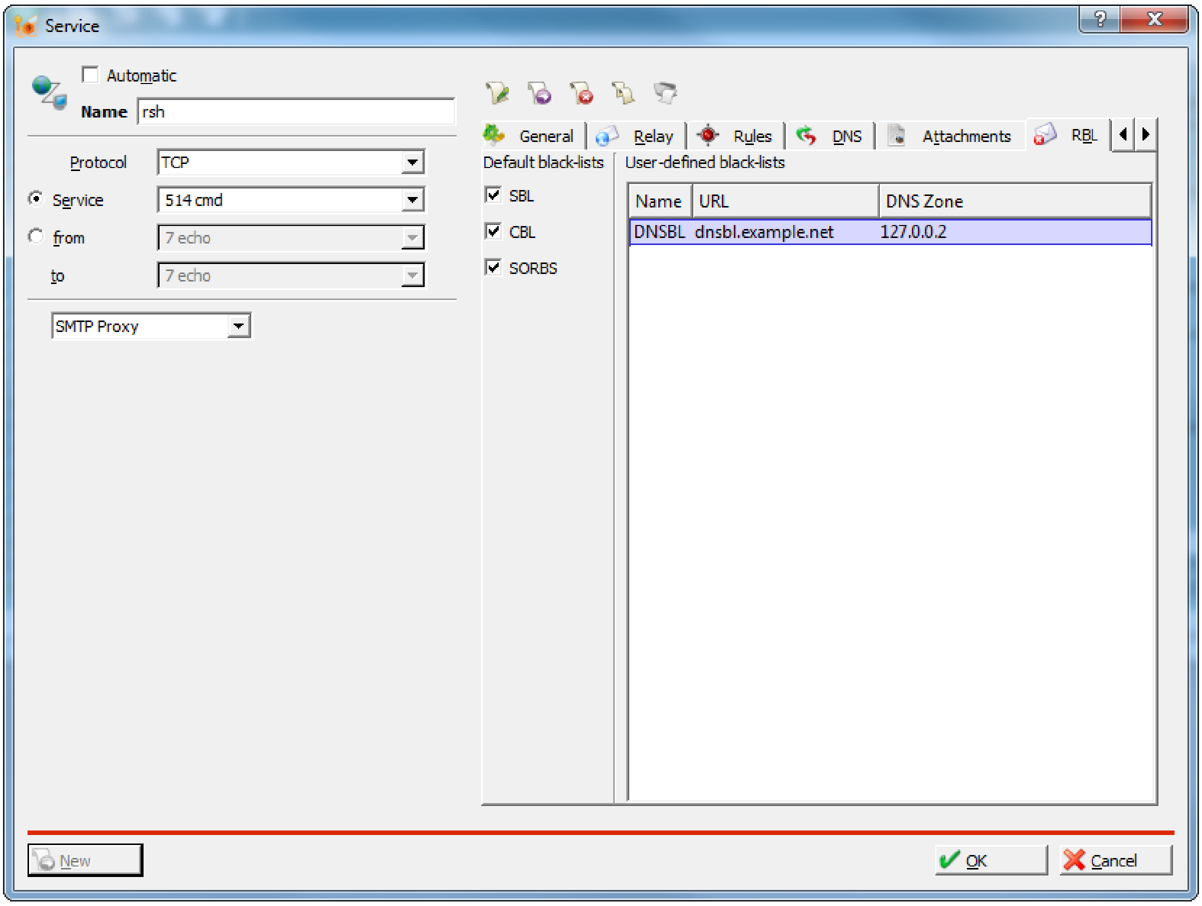
Notify sender if attachments are removed: If this option is checked, the firewall will send a message to the sender of an e-mail every time one or more of its attached files are removed.

Send copy to administrator if attachments are removed: If this option is checked, the firewall will send a copy of all removed files to the administrator. If it is checked, one of the following sending options must be chosen:

- **Default e-mail address:** The copy of the message is sent to the default e-mail address.

- **Other:** The copy of the message is sent to the address specified in the field on the right.

RBL tab (Real-time Black List)



☐ Automatic

Name rsh

Protocol TCP

● Service 514 cmd

○ from 7 echo

to 7 echo

SMTP Proxy

Default black-lists

☑ SBL

☑ CBL

☑ SORBS

User-defined black-lists

Name	URL	DNS Zone
DNSBL	dnsbl.example.net	127.0.0.2

Image 432 – Rule: edition rule and attachments.

This tab contains the blocking options for sites considered sources of SPAM. The blocking is performed on real-time, by consulting one or more dynamic blocking lists, maintained by third-parties. It consists of the following options:

Default black-lists: There are three black-lists that contain several hosts accused of being spammers. They are managed by organizations and the firewall just consults them before accepting each e-mail. Please enable the corresponding options if it is desired to use this feature.

- **SBL:** For more information access the address http://www.spamhaus.com
- **CBL:** For more information access the address http://cbl.abuseat.org
- **SORBS:** For more information access the address http://www.sorbs.net/

User-defined black-lists: These are black-lists configured by the firewall administrator. It consists of a list of black-lists, each one with the following fields:

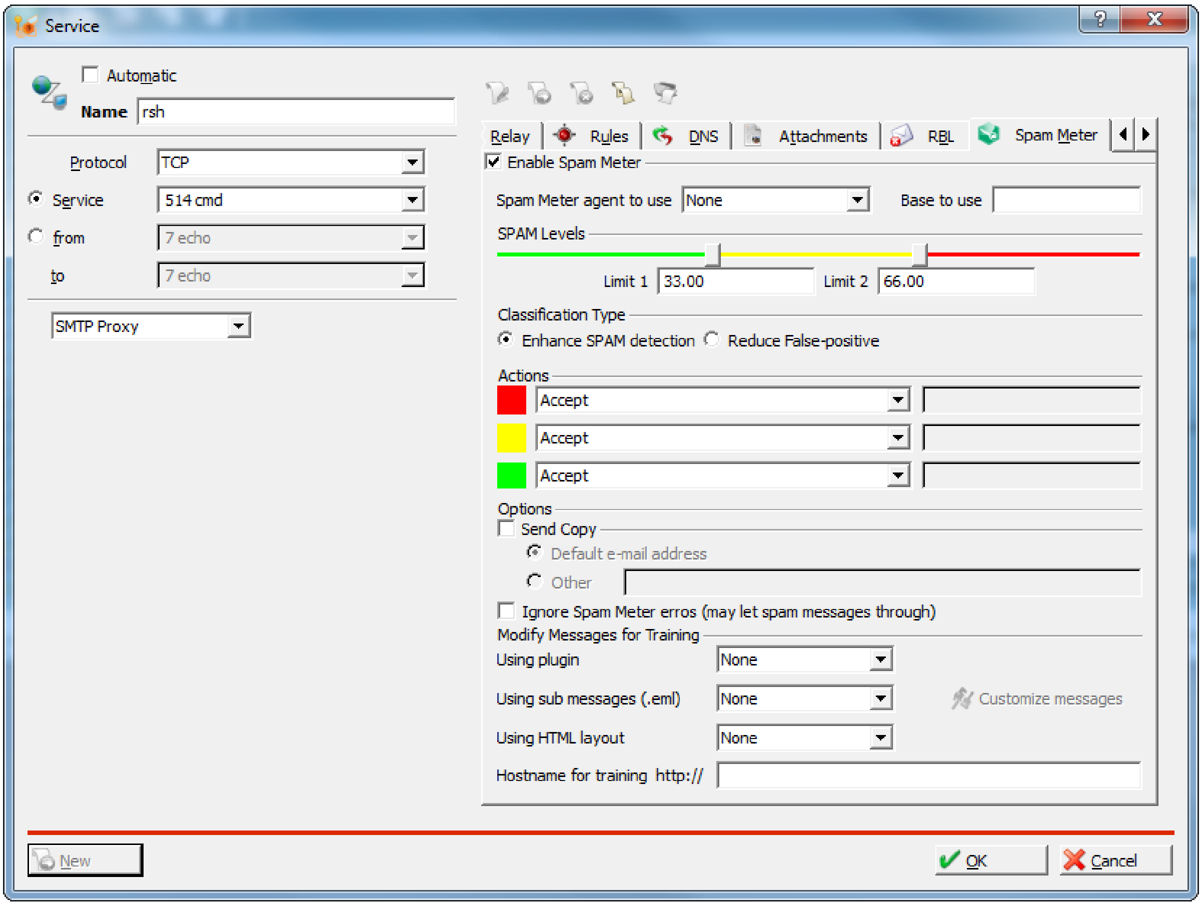
Name: Black-list name.

URL: It is the URL that will be displayed to the users that have their messages refused, so they can gather more information.

DNS Zone: It is the complete DNS zone that will be consulted by the firewall. If an IP address is present in that zone, e-mails from it will be refused by the firewall.

Some black-list services usually have their operation interrupted temporarily due to legal issues. When this happen they become ineffective and may block more senders than they should. Please check the correct black-list functioning before using it.

Spam Meter tab



☐ Automatic

Name: rsh

Protocol: TCP

● Service: 514 cmd

○ from: 7 echo

to: 7 echo

SMTP Proxy

☑ Enable Spam Meter

Spam Meter agent to use: None

Base to use:

Limit 1: 33.00

Limit 2: 66.00

Classification Type

● Enhance SPAM detection ○ Reduce False-positive

Actions

🟥 Accept

🟨 Accept

🟩 Accept

☐ Send Copy

● Default e-mail address

○ Other

☐ Ignore Spam Meter erros (may let spam messages through)

Modify Messages for Training

Using plugin: None

Using sub messages (.eml): None

Using HTML layout: None

Hostname for training http://

Image 433 – Service: Spam Meter.

This tab contains the Firewall communication configuration options with the Spam Meter, a product developed by Aker Security Solutions aiming to assign grades to email messages according to the probability of these messages be SPAM or not.

Enable Spam Meter: Enables the use of SPAM METER by the Firewall.

Spam Meter agent to use: This field indicates the Spam Meter that will be used to assign grades to email messages. This agent must be previously registered. For more information see the chapter titled **Registering Entities**.

Base to use: Spam Meter allows the use of several bases to perform the messages classification. The goal is allow each person or group of people with similar characteristics can have their messages classified by a better base that reflects their Spam definition. Aker Firewall does not allow the user of different bases by people or groups, but it is possible to use a distinct base for each SMTP context.

Spam Levels: This control allows defining two grades limits (between 0 and 100) to the messages filtering. These limits are named **Limit 1** and **Limit 2**, and the description of them follows below:

Limit 1: Defines the maximum limit (green strip) that the messages will be considered as not SPAM.

Limit 2: Defines together with the *Limit 1,* the yellow and red strips. The yellow strip represents emails that potentially are SPAMs, but the Spam meter is not 100% sure about it.

Enhance SPAM detection: If this option is selected the Spam Meter will attempt to detect the larger amount of SPAM messages, eventually more false-positive will be generated.

Reduce False-positive: If this option is selected, Spam Meter will reduce the maximum possible the *False-positive*, eventually messages that could be SPAM will be treated as harmless.

Action: This field indicates the actions that should be taken by the messages which fit in each one of the areas defined by the limits 1 and 2. The description of this option follows below:

Accept: Messages that fit in this strip will be accepted without any modification. Normally this action is associated to the green strip.

Discard: Messages that fit in this strip will be discarded by the firewall, i.e. these messages will be received by the server that has sent them will be notified about the successful delivery, however these messages will never be sent to users who should receive them.

Reject: Messages that fit in this strip will be rejected by Firewall, i.e. the serve that has sent these messages will be informed that they have been rejected and they should not send them again.

Add subject: Messages that fit in this string will be accepted, but will have their subject preceded by a text defined by the administrator. The field on the left is used by the administrator to define the text that will be added to the subject.

Send Copy: All message regardless of being accepted or rejected, is possible sending a complete copy of it to any email address. This field indicates if this copy should or not be sent. In case it is checked, one of the following options needs to be chosen:

- **Default e-mail address:** The copy of message is sent to the default email.
- **Other:** The copy of message is sent to the email specified in the field.

Modify Messages for Training Spam Meter can learn new characteristics of SPAM, in order to offer a greater hit level. The fields in this option indicate which users can perform the context database training and how the messages shall be modified in order to make the training possible. The following options are available:

Using plugin: This field indicates the recipients who will train their messages through the training plugin provided by Aker (available for Outlook and Thunderbird). In this case, the messages will not be modified; just new fields will be added in the header. It specifies an entity of type *email* that shall be previously registered in the firewall (for more information see chapter titled **Registering Entities**).

Using sub messages (.eml): The recipients located in this field will receive their original messages encapsulated in another, which will have buttons that will make possible the training (the initial message will have no change, but few readers will require user to click on it, in order to see it). It specifies an entity of type *email* that shall be previously registered in the firewall (for more information see chapter **Registering Entities**).

Using HTML layout: The recipients located in this field will receive their original messages together with a new HTML layout, which will contain buttons that will make possible the training. It specifies an entity of type *email* that shall be previously registered in the firewall (For more information see the chapter **Registering Entities**).

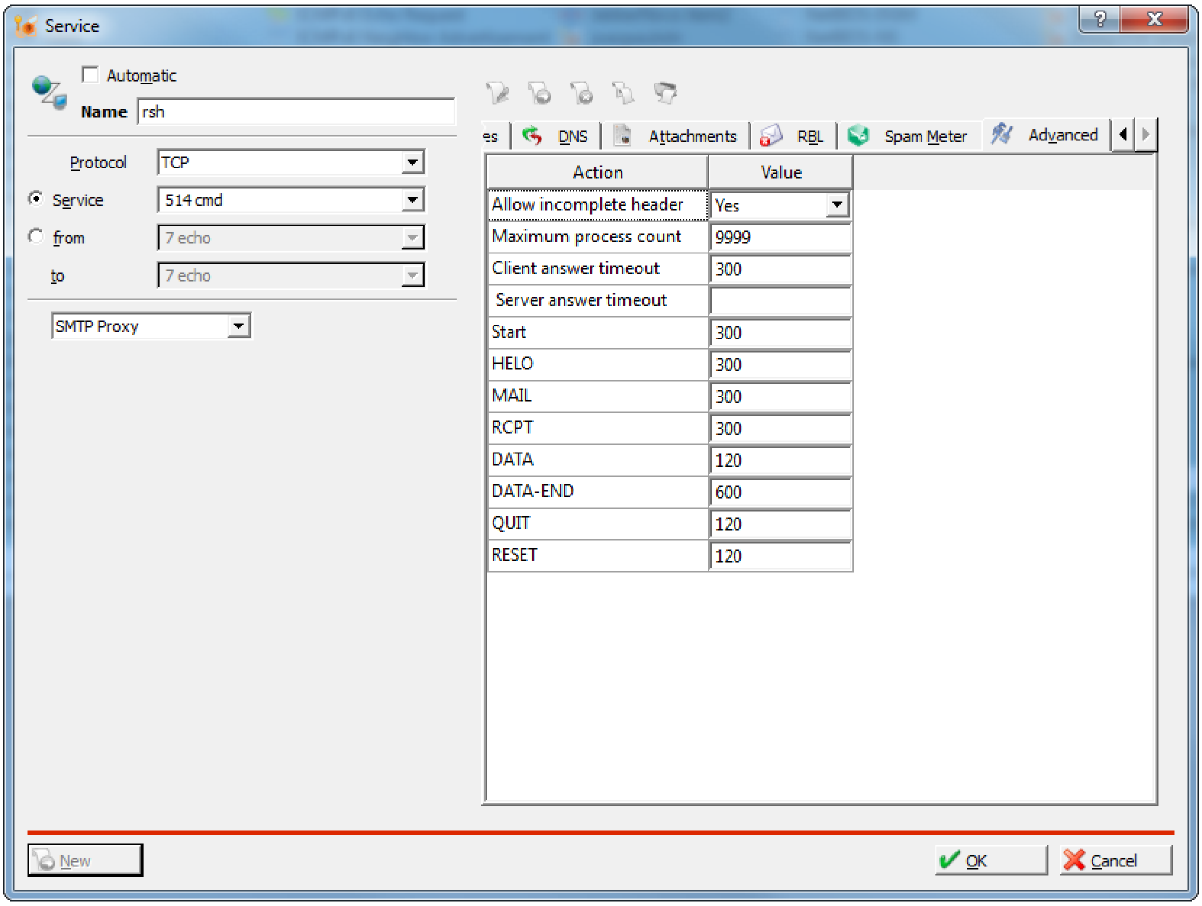
Customize messages: If one of these options **Using sub messages** or **Using HTML layout** is selected, this option will enabled and it will define what messages will be displayed to users so they can do the training.

Hostname for training: This field must to be filled in with name or Host IP address which the firewall is running on, so client email readers will know where send the training result to.

The lists will be searched by firewall in the same order that they are displayed, i.e. if a receiver is in two or more lists, the message will be modified according to the

In case a user does not appear in any list, this user will not be allowed to do the training.

Advanced tab



☐ Automatic

Name rsh

Protocol TCP

● Service 514 cmd

○ from 7 echo

to 7 echo

SMTP Proxy

Action	Value
Allow incomplete header	Yes
Maximum process count	9999
Client answer timeout	300
Server answer timeout	
Start	300
HELO	300
MAIL	300
RCPT	300
DATA	120
DATA-END	600
QUIT	120
RESET	120

Image 434 – Service: Advanced.

This tab allows access to the advanced configuration options of the SMTP proxy. They permit a fine tuning of the proxy. The options are:

Allow incomplete header: If this option is checked as NOT, messages whose headers do not contain all the mandatory fields of a SMTP message will be rejected.

Maximum process count: This field indicates the maximum number of copies of the proxy that can be active in a specific moment. Since each process handles a connection, this number also represents the maximum number of messages that can be sent simultaneously to the given context. If the number of active connections reaches this limit, hosts trying to send new messages will be informed that the server is temporarily unable to accept new connections and they should try later.

It is possible to use this number of processes like a tool to control the maximum number of messages passing through the link.

Server answer timeout: For each of the possible valid commands of the SMTP protocol, there is a maximum waiting time. If there is no answer within this period of time, the proxy assumes that the server has crashed and closes the connection. In this group it is possible to configure the maximum timeout, in seconds, for each one of these commands.

Client answer timeout: This parameter indicates the maximum time, in seconds, that a proxy waits between each command of the client that is sending the SMTP message. If this time is reached, without receiving any command from the client, the proxy assumes that the host has crashed and closes the connection.

All the remaining settings refer to timeouts for each SMTP command and they should not be modified unless there is a specific need to do so.

Configuring Telnet proxy

26. Configuring the Telnet proxy

This chapter shows how to configure the telnet proxy to perform the user authentication.

What is Telnet Proxy?

The Telnet Proxy is a special Aker Firewall program to work with the Telnet protocol. This protocol is used to emulate remote terminals. Its basic function is to enable user level authentication for telnet sessions. This type of authentication allows greater flexibility and higher security level.

It is a transparent proxy (for more information, see the chapter titled **Working with proxies**), therefore, neither the server, nor the client are aware of its existence.

Using the Telnet proxy

To perform authentications in a communication using the Telnet Proxy, it is necessary to follow these 2 steps bellow:

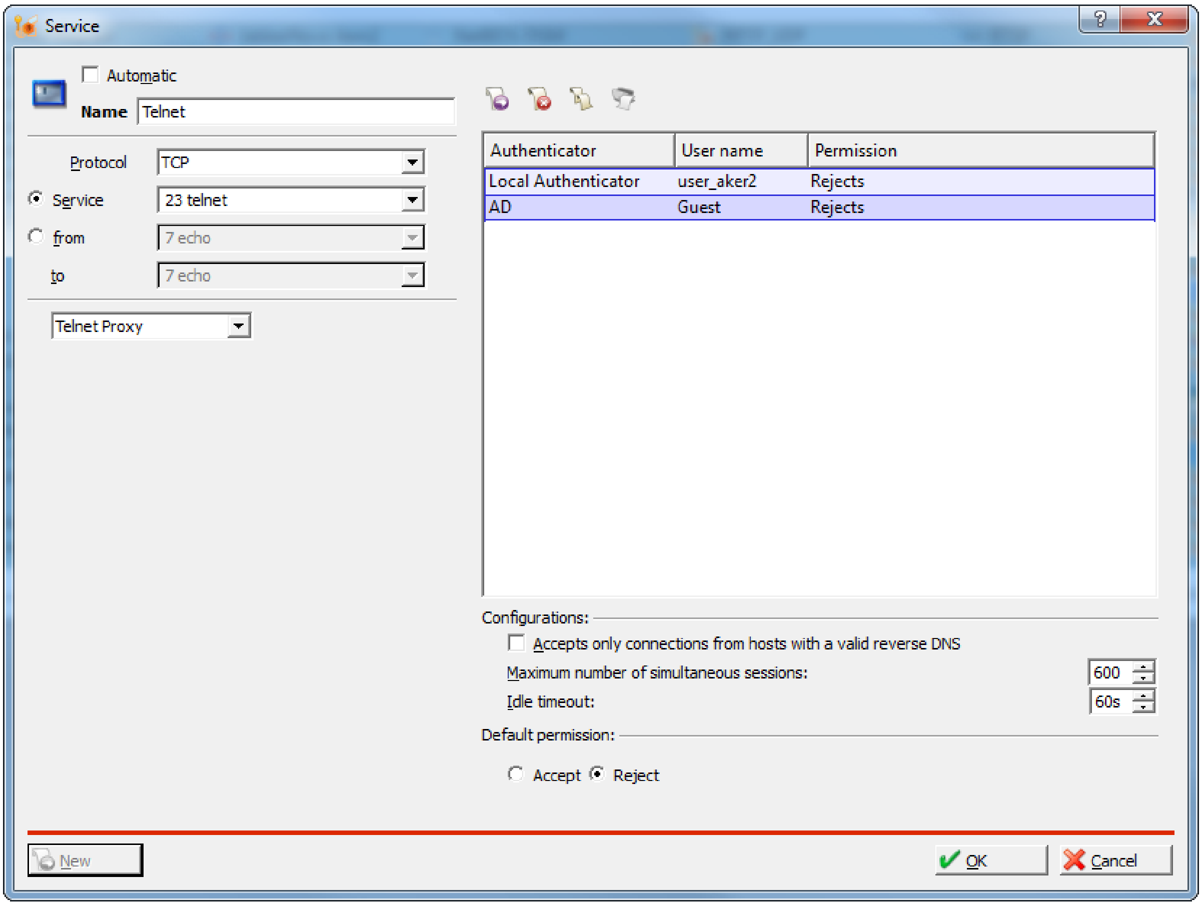
1. Create a service that will be redirected to the Telnet proxy and edit the context parameters that will be used by this service (for more information see the chapter titled **Registering Entities**).
2. Add a filtering rule allowing the use of this service by networks and desired hosts (for more information see the chapter titled **Stateful Filter**).

From now on, every time a Telnet session is established, matching the created rule, the firewall prompts for user identification and password. If identification and password are valid and the user does have permission, the session will be established. Otherwise, the user will be informed of the mistake, and the session canceled

26.1. Editing the parameters of a telnet context

The properties window of a Telnet context will be displayed when the **Telnet Proxy** option is selected. The behavior of the Telnet proxy, when it is dealing with a service, is defined here.

The properties window of a Telnet context



Service

☐ Automatic

Name Telnet

Protocol: TCP

● Service: 23 telnet

○ from: 7 echo

to: 7 echo

Telnet Proxy

Authenticator	User name	Permission
Local Authenticator	user_aker2	Rejects
AD	Guest	Rejects

Configurations:

☐ Accepts only connections from hosts with a valid reverse DNS

Maximum number of simultaneous sessions: 600

Idle timeout: 60s

Default permission:

○ Accept ● Reject

Image 435 – Service: propriedade de um contexto Telnet.

In the properties window are configured all context parameters associated with a specific service. It has the following fields:

Accept only connections from hosts with a valid reverse DNS: If this option is checked, only connections from hosts with configured reverse DNS, pointing to a valid name will be accepted.

Default Permission: This field indicates the permission applied to all users who are not present, and who are not included in any permission list group. There are two possible values. *Accept* allows establishment of Telnet session and *Reject* blocks it.

Maximum number of simultaneous sessions: This field defines the maximum number of Telnet sessions that may be simultaneously active in this context. If the number of open sessions reaches this limit, users trying to establish new connections will be informed about it and encouraged to try again later.

Idle timeout: Defines the maximum amount of time, in seconds, the proxy may remain idle without receiving data from the Telnet session, and still consider it active.

This field value must be less than, or equal to the value configured in the **TCP timeout** field, in the Global Configuration Parameters (for more information, see the chapter **Configuring system parameters**).

Permission List: This list defines individual user or group access permissions.

To execute any operation on a user or group in the Permission List, just right-click on it.

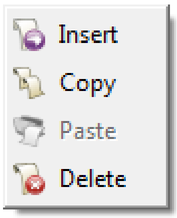


Image 436 – Option menu

- **Insert:** This option adds a new user/group to the list. If any user/group is selected, the new one will be inserted in its position, moving it down one position on the list. Otherwise, the new one will be added to the end of the list.
- **Edit:** This option changes the selected user/group access permission.
- **Delete:** Removes selected user/group from the list.

Hint: All these options may be executed from toolbar just above the list. In this case, first select the user/group by clicking on it, and then click on the desired toolbar option.

User/group order in the Permissions List is very important, because when a user is authenticated, the firewall searches the list from the beginning, looking for this user name, or for a group which this user belongs to. As soon as one is found, the associated permission is used.

To change a user/group position on the list, proceed as follows:

1. Select the user or group to change position.
2. Click on one of the arrow buttons, on the right. The up arrow button will move the user/group up one position. The down arrow button, one position down.

When adding users/groups, the following window will show up:

The User/Group Addition window

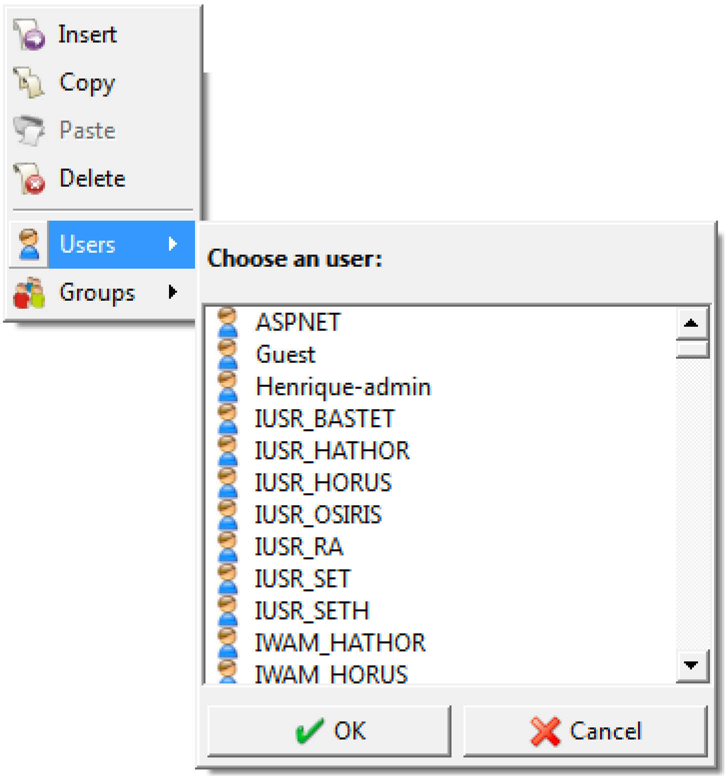

Insert
Copy
Paste
Delete
Users
Groups
Choose an user:
ASPNET
Guest
Henrique-admin
IUSR_BASTET
IUSR_HATHOR
IUSR_HORUS
IUSR_OSIRIS
IUSR_RA
IUSR_SET
IUSR_SETH
IWAM_HATHOR
IWAM_HORUS
OK
Cancel

Image 437 – Choosing a user.

The window is used to configure access permission for a user or group of a specific authenticator.

Select the authenticator which you wish to get the list of users or groups from, clicking on its name on the top list. (If it is not displayed on the list, first it is necessary to add it to the list of Authenticators to Query. For more information, see the chapter titled **Configuring authentication parameters**).

1. Select user or group list, clicking on the corresponding button located between the two lists.
2. On the bottom list, click on a user or group name you wish to add.
3. Choose the user/group access permission: accept (allows session establishment) or reject (blocks session establishment).
4. Click on **OK**. The window will be closed and the user/group will be added to the Permission List in the Context Properties window.

Configuring the FTP proxy

27. Configuring the FTP proxy

This chapter shows how configure FTP proxy blocking specifics commands of file transfer.

What is FTP proxy?

The FTP proxy is a specialized program of Aker Firewall, designed to work with the FTP protocol, which is the protocol used for file transfers in the Internet. Its basic function defines commands that can be accepted and blocked, for example, the creation of new files or directories.

It is a transparent proxy (for more information see the chapter titled **Working with proxies**), so nor client, nor server knows about its existence.

Using the FTP proxy

To use the FTP proxy to perform the file transfer control is necessary to do the following steps:

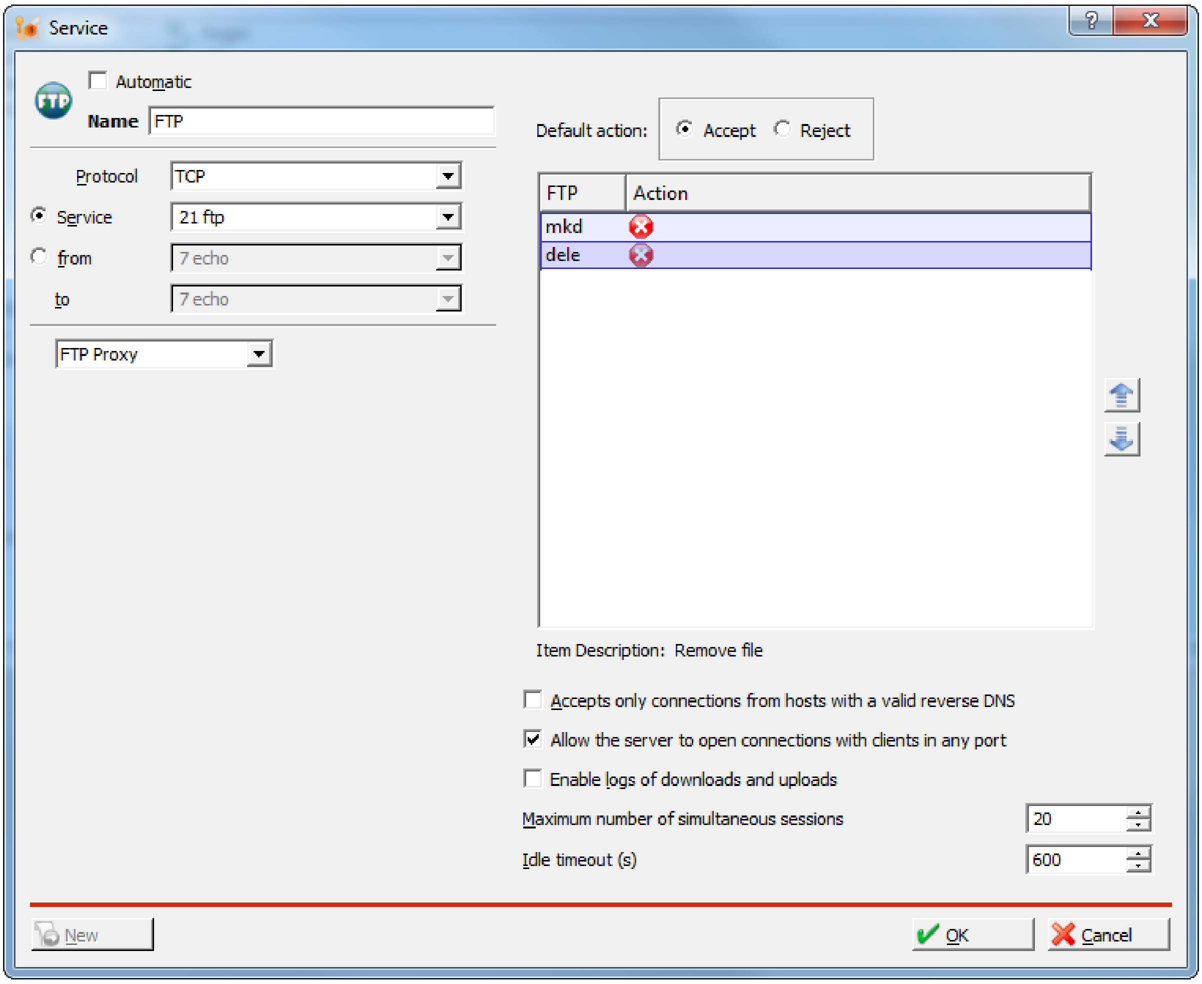
1. Create a service which will be redirected to the FTP proxy and edit the parameters of the context to be used for this service (for more information see the chapter titled **Registering Entities**).
2. Add a filtering rule to enable the use of the service created in step 1, for the desired networks or hosts (for more information see the chapter titled **Stateful Filter**).

The FTP proxy does not perform user authentication. To allow certain users to have different privileges, it is necessary to create proxy FTP services with different contexts and associate each of these services with an access profile. For more information about access profiles see the chapter titled *User access profiles*.

27.1. Editing the parameters of a FTP context

The properties window of a FTP context is displayed when the **FTP Proxy** option is selected, in the services edition window. Through this window it is possible to define the behavior of the FTP proxy when dealing with a specific service.

FTP context configuration window



☐ Automatic

Name FTP

Protocol TCP

● Service 21 ftp

○ from 7 echo

to 7 echo

FTP Proxy

Default action: ● Accept ○ Reject

FTP	Action
mkd	✖
dele	✖

Item Description: Remove file

☐ Accepts only connections from hosts with a valid reverse DNS

☑ Allow the server to open connections with clients in any port

☐ Enable logs of downloads and uploads

Maximum number of simultaneous sessions 20

Idle timeout (s) 600

Image 438 – Services: FTP context configuration window.

The properties window is where all parameters of a context, associated to a specific service, are configured. It consists of the following fields:

Accepts only connections from hosts with a valid reverse DNS : When this option is selected, only connections from hosts with a configured reverse DNS, pointing to valid name, will be accepted.

Allow the server to open connections with clients in any port: This option allows the FTP server communicate with client through a port which is not the default TCP20.

Enable logs of downloads and uploads: This option will generate an event informing the data about downloads and uploads done through proxy.

Maximum number of simultaneous sessions: This field defines the maximum number of FTP sessions that can be simultaneously active in this context. If the number of open sessions reaches this limit, the users who try to establish new connections will be informed that the limit has been reached and that they should try again later.

Idle timeout: This item defines the maximum amount of time, in seconds, that the proxy can stay without receiving data from the FTP session and still consider it active.

The value of this field should be less or equal to the value configured in the **TCP Timeout** field, on the global configuration parameters (for more information see the chapter titled **Configuring the system parameters**).

This window allows creating a list of rules that might be **accepted** or **rejected**, according to the icon in the **Action** column.

To add a command in the FTP column simply right-click in the blank area and select **Insert**. To change the command you shall click on it a select one of the following options:

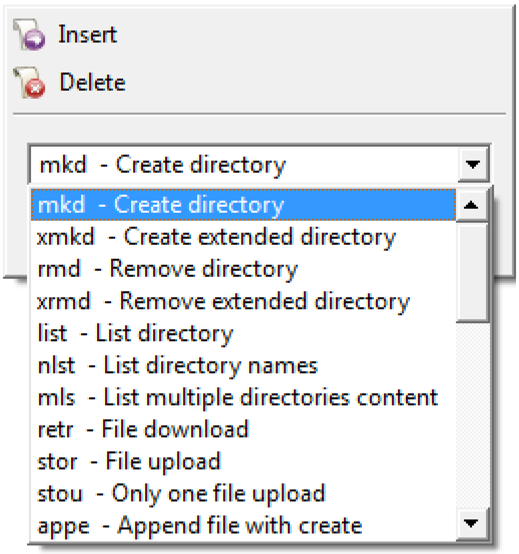

Insert
Delete
mkd - Create directory
mkd - Create directory
xmkd - Create extended directory
rmd - Remove directory
xrmd - Remove extended directory
list - List directory
nlst - List directory names
mls - List multiple directories content
retr - File download
stor - File upload
stou - Only one file upload
appe - Append file with create

Image 439 – Rules list.

Below follows the description of each one of them:

mkd – Create directory: Selecting this option you will be able to create directories through FTP connections that fit in this context.

xmkd – **Create extended directory:** Selecting this option you will be able to create extended directories through FTP connections that fit in this context.

rmd – Remove directory: Selecting this option you will be able to remove directories through FTP connections that fit in this context.

xrmd – Remove extended directory: Selecting this option you will be able to remove extended directories through FTP connections that fit in this context.

list – List directory: Selecting this option you will be able to view the directories content through FTP connections that fit in this context.

nlst – List directory names: Selecting this option you will be able to view the directories names through FTP connections that fit in this context.

retr – File Download: Selecting this option you will be able to download files through FTP connections that fit in this context.

stor – File upload: Selecting this option you will be able to upload files through FTP connections that fit in this context.

stou – Only one file upload: Selecting this option you will be able to upload a unique file in the current directory.

appe – Append file with create: Selecting this option you will be able to append the data a file. If this file does not exist, one will be created.

rest – Resume file transfer: Selecting this option you will be able to resume a download or upload where it has been stopped.

dele – Remove file: Unchecking this option you will not be able to remove files through FTP connections that fit in this context.

rnfr – Rename file: Selecting this option you will be able to rename files through FTP connections that fit in this context.

The rules not presented above will perform the “default action”.

Configuring POP3 proxy

28. Configuring the POP3 proxy

This chapter shows what functions are offered by POP3 proxy and how to configure it.

What is the POP3 proxy?

The POP3 proxy is a special Firewall Aker program, designed to work with email (POP3 is an acronym for *Post Office Protocol*, which is the full name of the service that downloads email messages in the Internet). This proxy enables email filtering based on their attachment files. It also acts as a shield, protecting the POP3 server against several types of attacks.

It is a transparent proxy (for more information, see the chapter titled **Working with Proxies**), thus, neither the server nor the client are aware of its existence.

Attacks against a POP3 Server

There are several types of possible attacks against a POP3 server, below follows the description of some of them:

- **Attacks that explore *bugs* in a server**

  In this case, the attacker tries to use a command or command parameter that causes security failures.

  Aker Firewall POP3 proxy avoids these attacks because it only allows utilization of commands considered secure, and it validates all commands parameters.

- **Attacks that explore buffers overflow**

  These attacks consist of sending very long command lines to a server, which, when not correctly developed, will present security failures.

  Aker Firewall POP3 proxy blocks these attacks by limiting command line length that may be sent to the server.

Using the POP3 proxy

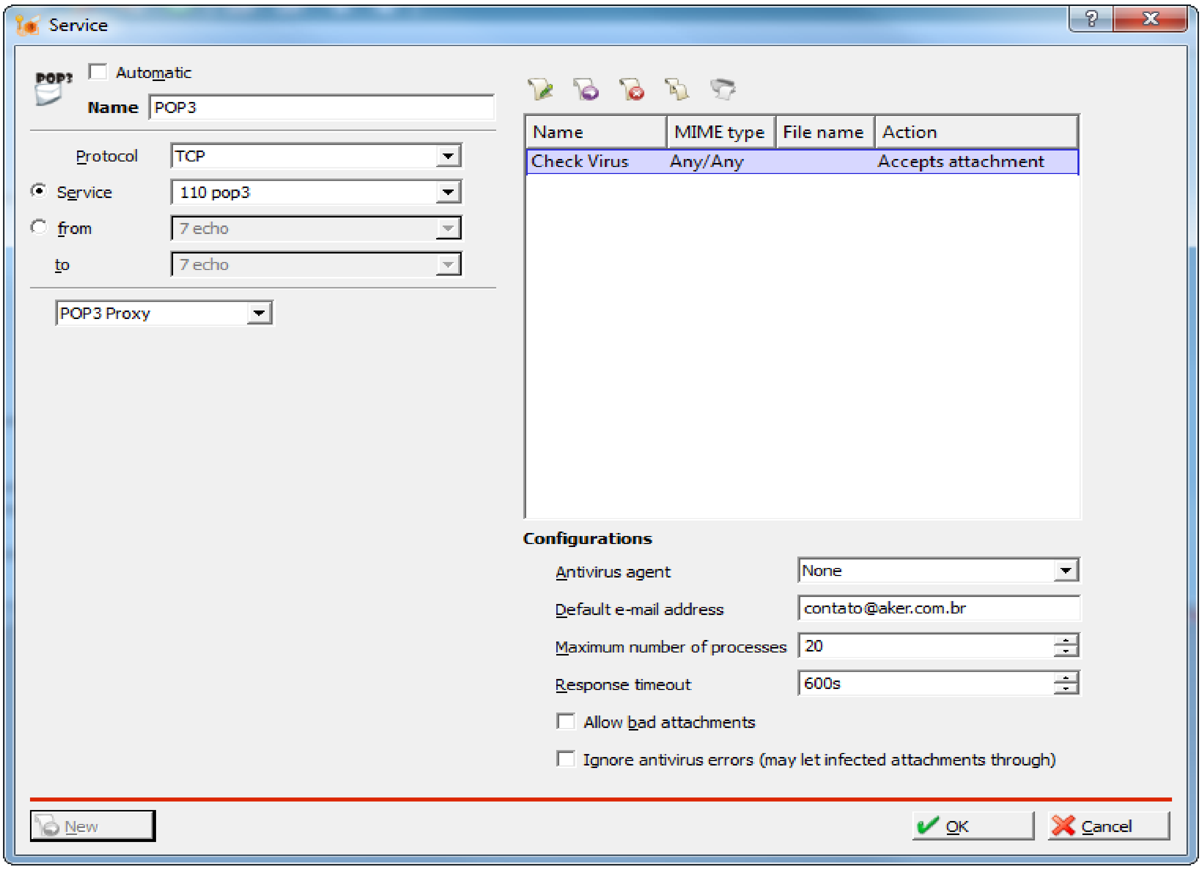
To use the POP3 proxy in a communication, two steps are necessary:

1. Create an entity of type *Service* that will be redirected to the POP3 proxy, and edit the context parameters that will be used by this service (for more information, see the chapter **Registering Entities**).
2. Add a filtering rule allowing the use of the service created in step 1 by the networks or desired hosts (for more information, see the chapter **Stateful Filter**).

28.1. Editing parameters of a POP3 context

When the **POP3 Proxy** option is selected, the POP3 Context Properties window shows up. In this window, we configure the POP3 Proxy behavior for the service being created.

POP3 Context configuration window



☐ Automatic

Name: POP3

Protocol: TCP

● Service: 110 pop3

○ from: 7 echo

to: 7 echo

POP3 Proxy

Name	MIME type	File name	Action
Check Virus	Any/Any		Accepts attachment

Configurations

Antivirus agent: None

Default e-mail address: contato@aker.com.br

Maximum number of processes: 20

Response timeout: 600s

☐ Allow bad attachments

☐ Ignore antivirus errors (may let infected attachments through)

Image 440 – POP3 configuration window.

All parameters of a context associated to a specific service are configured in the Properties window. They are:

Configurations: It is made up of several fields that indicate actions to be performed by the POP3 proxy.

- **Antivirus agent:** This field identifies the antivirus agent that will be used to check e-mail attachments. This agent must have been previously registered in the firewall. For more information, see the chapter titled **Registering Entities**.
- **Default e-mail address:** Indicates the default e-mail address where copies of all messages that do not match any of the context rules will be sent to (if the option **Send Copy** is checked). This e-mail can also be used in any context filtering rule.
- **Maximum number of processes:** This field indicates the maximum number of proxy copies that can be active at a given time. Because each process deals with a connection, this number also represents the maximum number of messages that can be simultaneously transmitted to that specific context. If the number of active connections reaches this limit, clients trying to send new messages will have to try again at a later time.
- **Response timeout:** This parameter indicates the maximum amount of time, in seconds, that the proxy waits for an idle connection. If this time is reached, the proxy terminates the connection.
- **Let bad attachments go through:** Allows corrupted attachments to pass through the firewall into mailboxes.

List of rules: In this list filtering rules for attachments are specified, determining whether a message will have its attachments removed or scanned for viruses.

To perform any operation on a specific rule, just right-click on it. The following menu shows up: (This menu will always show up when the right mouse button is pressed, even if no rule is selected. In this case, just the *Insert* and *Paste* options will be enabled).

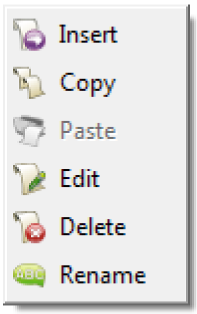


Image 441 – Option menu.

- **Insert**: This option adds a new rule to the list. If any rule is selected, the new one will be inserted in its position, pushing it down the list. Otherwise, the new rule will be added in the end of the list.

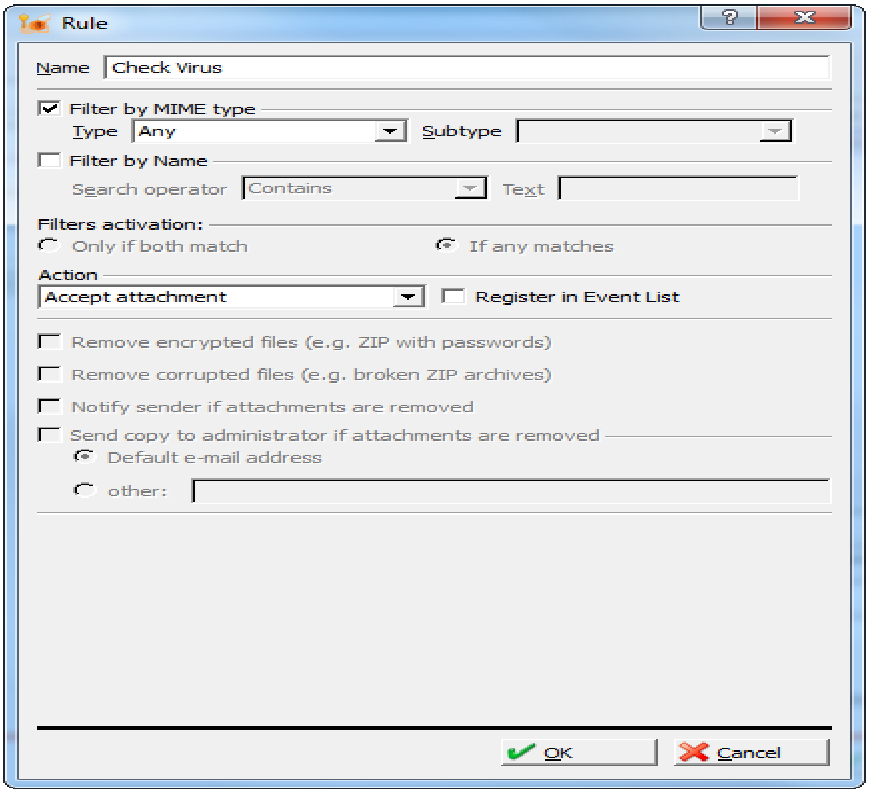
- **Edit**: This option opens the editing window for the selected rule.
- **Delete**: Removes the selected rule from the list.
- **Copy**: This option copies the selected rule into a temporary area.
- **Paste**: This option copies the rule from the temporary area into the list. If any rule is selected, the new one will be copied into its position, pushing it down. Otherwise, it will be copied at the end of the list.
- **Rename**: This option renames the selected rule.

Hint: All these options may be executed from the toolbar just above the list. First select the rule and then click on the desired option.

The order of the attachment filtering rules is extremely important. For each message attachment, the firewall searches the list from the beginning, looking for a matching rule. As soon as a match is found, the associated action is executed.

The window below shows up when rules are being added or edited:

File rules configuration



Name: Check Virus

☑ Filter by MIME type

Type: Any

Subtype:

☐ Filter by Name

Search operator: Contains

Text:

Filters activation:

○ Only if both match

● If any matches

Action: Accept attachment

☐ Register in Event List

☐ Remove encrypted files (e.g. ZIP with passwords)

☐ Remove corrupted files (e.g. broken ZIP archives)

☐ Notify sender if attachments are removed

☐ Send copy to administrator if attachments are removed

● Default e-mail address

○ other:

Image 442 – Rules configuration.

All parameters concerning attachment filtering rules for a POP3 context are configured in this window. It has the following fields:

Name: Name that uniquely identifies the rule within the context. This name will be displayed in the rules list. There cannot be two rules with the same name.

Filter by MIME type: This field allows definition of a file filtering rule based on its MIME type. When selected, type and subtype must be specified.

Filter by Name: This field allows filtering by the name of attached file (or part of it). When checked, the type of search to be performed and the text to be searched must be provided. The following search options are available:

- **CONTAINS**: The name must contain the supplied text in any position.
- **DOESN'T CONTAIN**: The name must not contain the supplied text.
- **IS**: The content of the name must be exactly equal to the supplied text.
- **IS NOT**: The content of the name must be different of the supplied text.
- **STARTS WITH**: The name must start with the supplied text.
- **DOESN'T START WITH**: The name must not start with the supplied text.
- **ENDS WITH**: The name must end with the supplied text.
- **DOESN'T END WITH**: The name must not end with the supplied text.
- **CONTAINS WORDS**: In this type of search, the supplied text is considered as formed by individual words (separated by spaces), instead of a continuous text. To match the search, the name must contain all the given words, regardless of their positions.

Filters Activation: If the option **Filter by MIME type,** and **Filter by Name** have been selected, this field determines if the rule must be applied **Only if both match** (**AND** value) or **If any one matches** (**OR** value).

Action: Indicates action to be taken by the firewall when a file matches the rule. It has three options:

- **Accept attachment:** If this option is selected, the firewall will keep the file attached to the message.
- **Remove attachment**: If this option is selected, the firewall will remove the attached file from the message.
- **Remove infected attachment:** If this option is selected, the firewall will check the attachment for virus. If the file is infected, the firewall will either: if the file can be disinfected, remove the virus and attach the file back to the message. If the file cannot be disinfected, the firewall will remove the attachment and add a message informing the recipient of its action.

If the **Register in Event List** box is checked, rule matches will be registered in the events log.

Remove encrypted files: The firewall will remove zipped with passwords and encrypted attachments, because it will not be able to scan them for viruses.

Remove corrupted files: If this option is checked, the firewall will remove zipped attachments that are corrupted, once it will not be able to scan them for viruses.

Notify sender if attachments are removed: The firewall sends a message to the message sender every time one or more of its attachments are deleted.

Send copy to administrator if attachments are removed: The firewall sends a copy of all deleted attachments to the administrator. If this option is selected, one of the following options must be chosen.

- **Default e-mail address:** The copy of the message is sent to the default e-mail, defined in the Context Properties window.
- **Other**: The copy of the message is sent to the address specified in the field to the right.

Using Quotas

29. Using Quotas

This chapter shows how the Quotas are used.

What are quotas?

Employees' productivity is of fundamental importance for the development and the growth of a company. Therefore, your network resources should be used rationally. Due to it, Aker Firewall has become an essential tool to control the access to web pages that users will have access within the limits established by the access quotas. Quotas are used to control and rationalize the time spent by users with access to web sites, this way the quotas are the limits the access time and data volume per user, these limits are defines in the following way:

- Regarding to the frequency of access, it can be set daily, weekly and monthly;
- Regarding to the amount of hours and available days;
- Regarding to the amount of data bytes transferred.

Note 1:

Web Filter: Quota consumption – The calculated time is approximately the same time taken to load a website.

MSN: Quota consumption – the calculated time is approximately the same time used in the MSN messenger, like chat, file transfer, games, videos call or any other MSN function.

Note 2:

Web Filter: For simultaneous access (from the same user) only the loading time of the larger website will be counted.

MSN: For each chatting window, the time will be counted separately;

29.1. Editing parameters of Quota usage

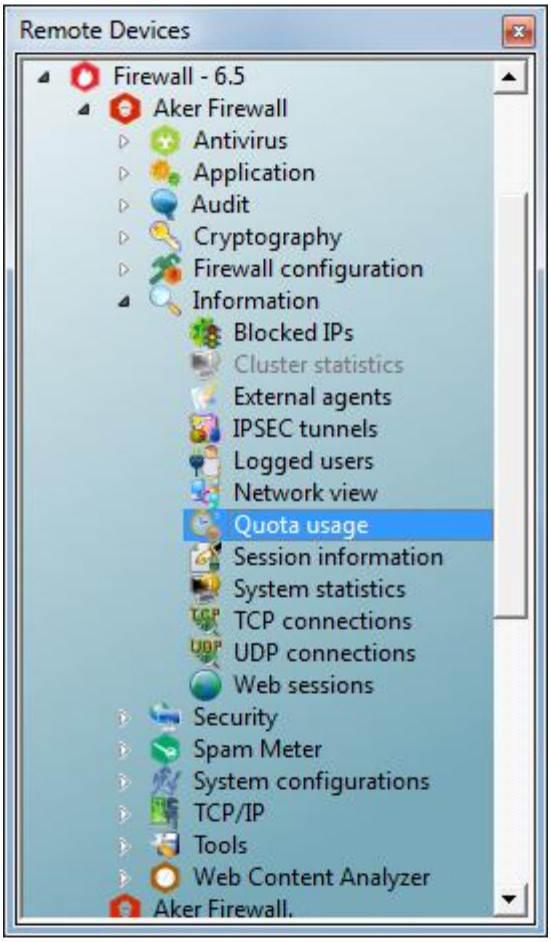
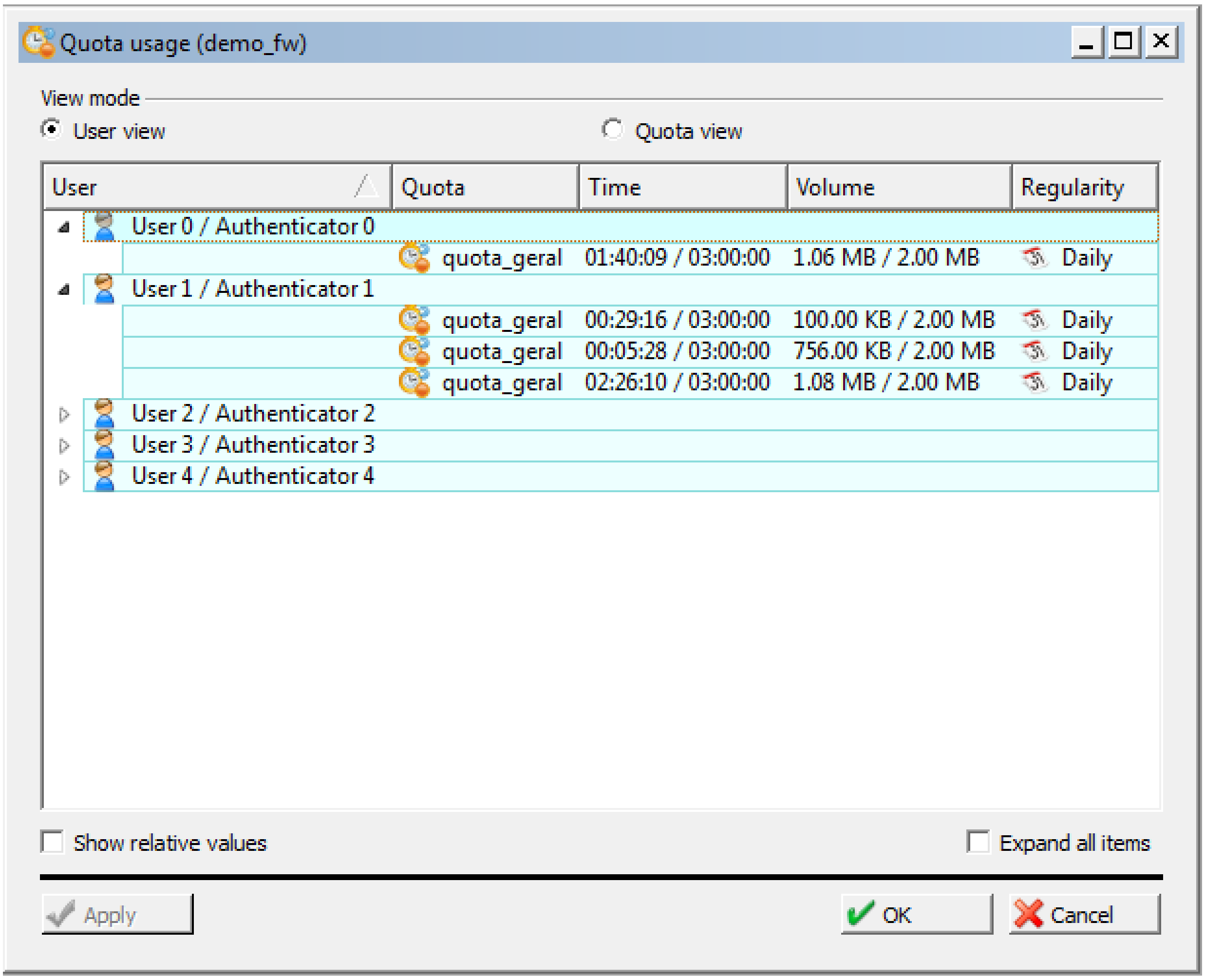

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Aker Firewall.

Image 443 – Access window: Quota usage.

- Click on the *Information* menu.
- Select *Quota usage*.

User view



View mode
● User view ○ Quota view

User	Quota	Time	Volume	Regularity
User 0 / Authenticator 0				
	quota_geral	01:40:09 / 03:00:00	1.06 MB / 2.00 MB	Daily
User 1 / Authenticator 1				
	quota_geral	00:29:16 / 03:00:00	100.00 KB / 2.00 MB	Daily
	quota_geral	00:05:28 / 03:00:00	756.00 KB / 2.00 MB	Daily
	quota_geral	02:26:10 / 03:00:00	1.08 MB / 2.00 MB	Daily
User 2 / Authenticator 2				
User 3 / Authenticator 3				
User 4 / Authenticator 4				

☐ Show relative values ☐ Expand all items

Image 444 – Quota usage: user view.

This window shows all quota information, specified per user.

Reset time for user: By right-clicking on the user and select this option, will reset all quota time for all quotas of this user. In case you click on the quota instead of clicking on the user, only the selected quota will have its time reset.

Reset traffic for user: By right-clicking on the user and select the option, will reset all data traffic of this user. In case you click on the *quota* instead of clicking on the *user,* only the selected quota will have its data traffic reset.

Reset time and traffic for user: By right-clicking on the user and select this option, will reset all time and traffic data for this user. In case you click on the quota instead of clicking on the user, only this specific quota will have its time and data traffic reset.

User: User which the quota has been applied.

Quota: Quota’s name.

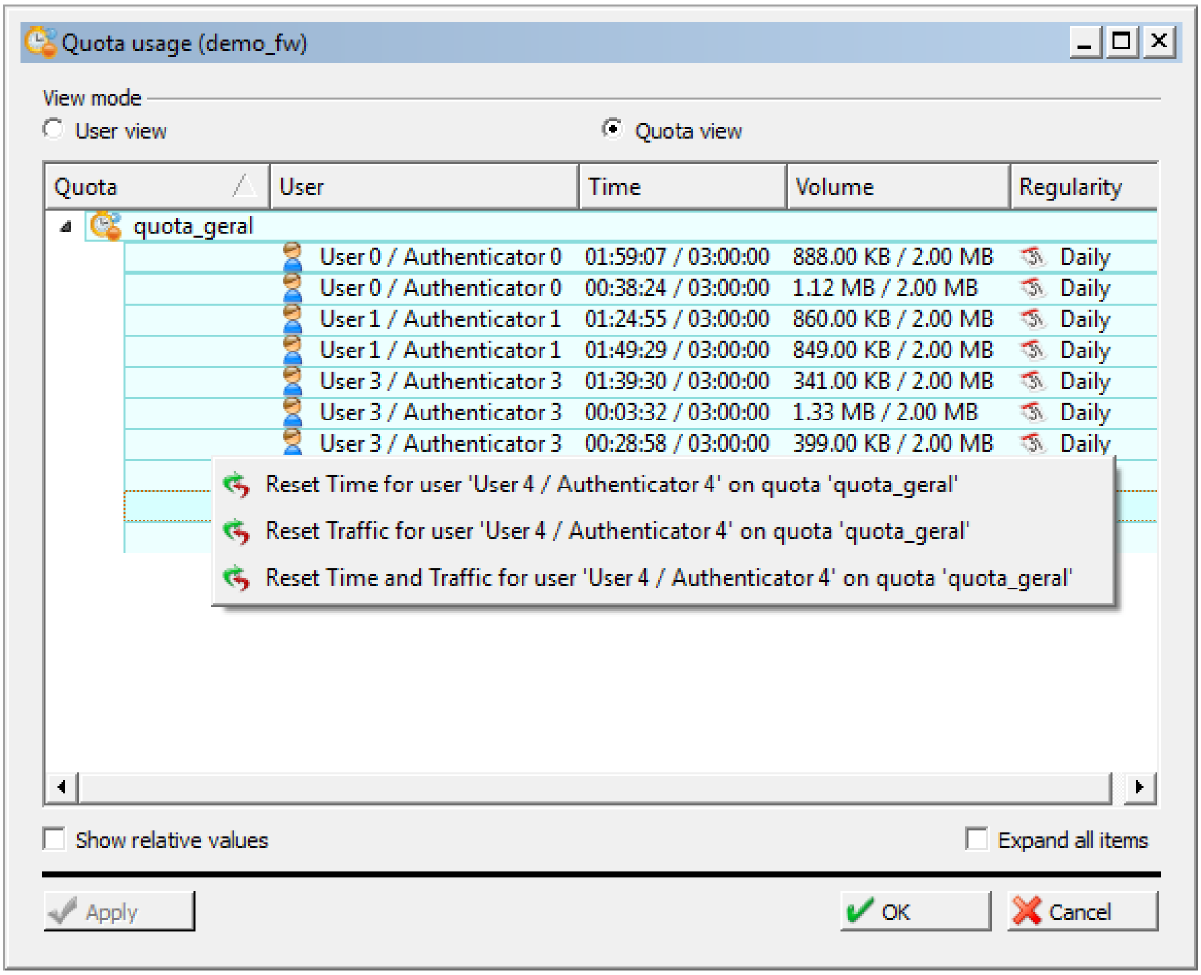
Time: Time spent by quota.

Volume: Amount of bytes transferred.

Regularity: Period that the quota will be applied daily, weekly or monthly.

Show relative values: Shows the used quotas values in percentage.

Quota view



View mode
○ User view ● Quota view

Quota	User	Time	Volume	Regularity
quota_geral				
	User 0 / Authenticator 0	01:59:07 / 03:00:00	888.00 KB / 2.00 MB	Daily
	User 0 / Authenticator 0	00:38:24 / 03:00:00	1.12 MB / 2.00 MB	Daily
	User 1 / Authenticator 1	01:24:55 / 03:00:00	860.00 KB / 2.00 MB	Daily
	User 1 / Authenticator 1	01:49:29 / 03:00:00	849.00 KB / 2.00 MB	Daily
	User 3 / Authenticator 3	01:39:30 / 03:00:00	341.00 KB / 2.00 MB	Daily
	User 3 / Authenticator 3	00:03:32 / 03:00:00	1.33 MB / 2.00 MB	Daily
	User 3 / Authenticator 3	00:28:58 / 03:00:00	399.00 KB / 2.00 MB	Daily

Reset Time for user 'User 4 / Authenticator 4' on quota 'quota_geral'
Reset Traffic for user 'User 4 / Authenticator 4' on quota 'quota_geral'
Reset Time and Traffic for user 'User 4 / Authenticator 4' on quota 'quota_geral'

☐ Show relative values ☐ Expand all items

Image 445 – Quota usage: quota view.

This window shows all quota information, specified per user.

Reset time for user: By right-clicking on the user and select this option, will reset all quota time for all quotas of this user. In case you click on the quota instead of clicking on the user, only the selected quota will have its time reset.

Reset traffic for user: By right-clicking on the user and select the option, will reset all data traffic of this user. In case you click on the *quota* instead of clicking on the *user,* only the selected quota will have its data traffic reset.

Reset time and traffic for user: By right-clicking on the user and select this option, will reset all time and traffic data for this user. In case you click on the quota instead of clicking on the user, only this specific quota will have its time and data traffic reset.

User: User which the quota has been applied.

Quota: Quota’s name.

Time: Time spent by quota.

Volume: Amount of bytes transferred.

Regularity: Period that the quota will be applied daily, weekly or monthly.

Show relative values: Shows the used quotas values in percentage.

Configuring Web filter

30. Configuring Web filter

This chapter shows what is and how to configure the Web fitter.

30.1. Planning the installation

What is Aker Firewall Web filter?

Web Filter is a specialized program of Aker Firewall to work together with the protocols that make part of the WWW (*World Wide Web*). Among these protocols are HTTP, HTTPS, FTP and Gopher.

This program main function is control the internal users access to the Internet, defining which pages the users can access , if the may or may not transfer files, etc. Besides it, Web Filter can block technologies considered dangerous for some installations like the Active-X^{TM,} scripts (JavaScript) and even Java Applets, and also allows the removal of banners of pages in order to increase your load speed, reduce the link use.

It is a transparent (only for HTTP) and non-transparent proxy at the same time (for more information see the chapter title **Working with proxies**), facilitating the system installation.

Using the transparent proxy is faster than the non-transparent proxy, besides it is not necessary any extra configuration on clients. In other hand to filter URLs for protocols HTTPS, FTP and GOPHER is possible only with the active proxy.

To a non-transparent proxy obtain the same performance as the transparent proxy, it is required that the browsers support the sending of HTTP 1.1 requests via proxies.

What is a cache server?

A cache server is a dedicated network server or service acting as a server that saves Web pages or other Internet content locally. By placing previously requested information in temporary storage, or cache, a cache server both speeds up access to data and reduces demand on an enterprise's bandwidth. Cache servers also allow users to access content offline, including rich media files or other documents. A cache server is sometimes called a "cache engine."

A cache server is almost always also a proxy server, which is a server that "represents" users by intercepting their Internet requests and managing them for users.

Aker Firewall Web Filter working with a cache server

Aker Firewall implements automatically a cache server in its Web Filter. This cache server can be in your machine or in another machine. In case you are using the cache server in another machine which is not yours (Installation mode is recommended) this machine must be in a different subnetwork from where the client machines are, otherwise all security control can be easily broken. Bellow follows the configuration:

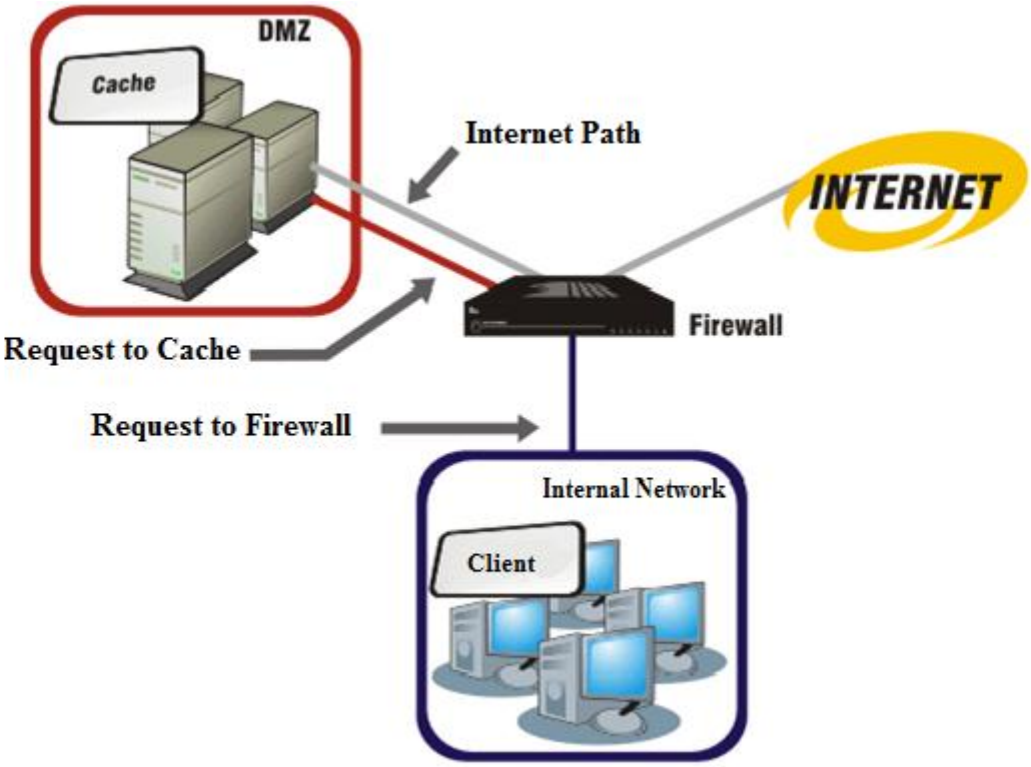


Image 446 – Connection (Internet, Intranet, firewall and DMZ)

To ensure total protection in this installation, simply configure the Stateful filter in order to allow the hosts with cache be the only one to access the services linked to WWW (*World Wide Web*), and the client hosts do not be allowed to open any connection towards the host where the cache is. Done with this, configure all client hosts to use the firewall Web Filter, and configure the firewall to use the cache on the desired machine (**for more information see the chapter titled Stateful Filter**).

Using the Web Filter

To use Aker Firewall Web Filter in non-transparent mode, follow the steps below:

1. Create the desired access profiles, and associate them to users and groups of your choice. (It has been describe in the chapter titled **User access profile**);
   2. Edit the Web Filter configuration parameters (it is going to be displayed in the chapter titled **Editing Web Filter parameters**);
3. Create a filtering rule granting the client hosts access to the proxy (for more information see the chapter titled **Stateful inspection**).

The non-transparent Web Filter listens to port 80 using the TCP protocol. If necessary this value can be changed to any port. Simply adding the parameter "-p", the port location and the port number you want the non-transparent Web Filter listens to, when it be iniciated. The command line that need to be changed is located in the file */aker/bin/firewall/rc.aker*, and it need to be changed from */aker/bin/firewall/fwhttppd to /aker/bin/firewall/fwhttppd -p 8080*, as example.

To use Aker Firewall Web Filter transparent mode, follow the steps below:

1. Create a service that will be disabled for the transparent Web Filter (HTTP and/or HTTPS) and edit the context parameters to be used by this service (for more information see the chapter titled **Registering Entities**).
2. Add a filtering rule allowing the created service in the step above, to be used for networks and hosts of your choice (for more information see the chapter titled **Stateful inspection**).

30.2. Editing the Web Filter parameters

To use the Web Filter is necessary to define few parameters that will determine basic characteristics of its operation. This definition is made in the Web Filter configuration window, to gain access to it follow the steps bellow:

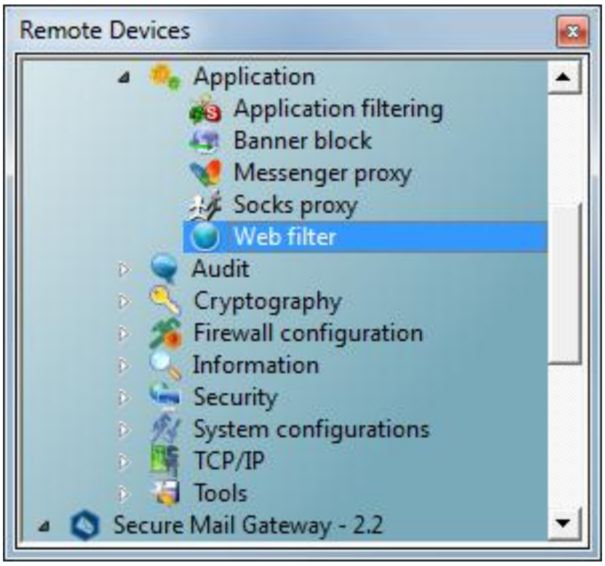
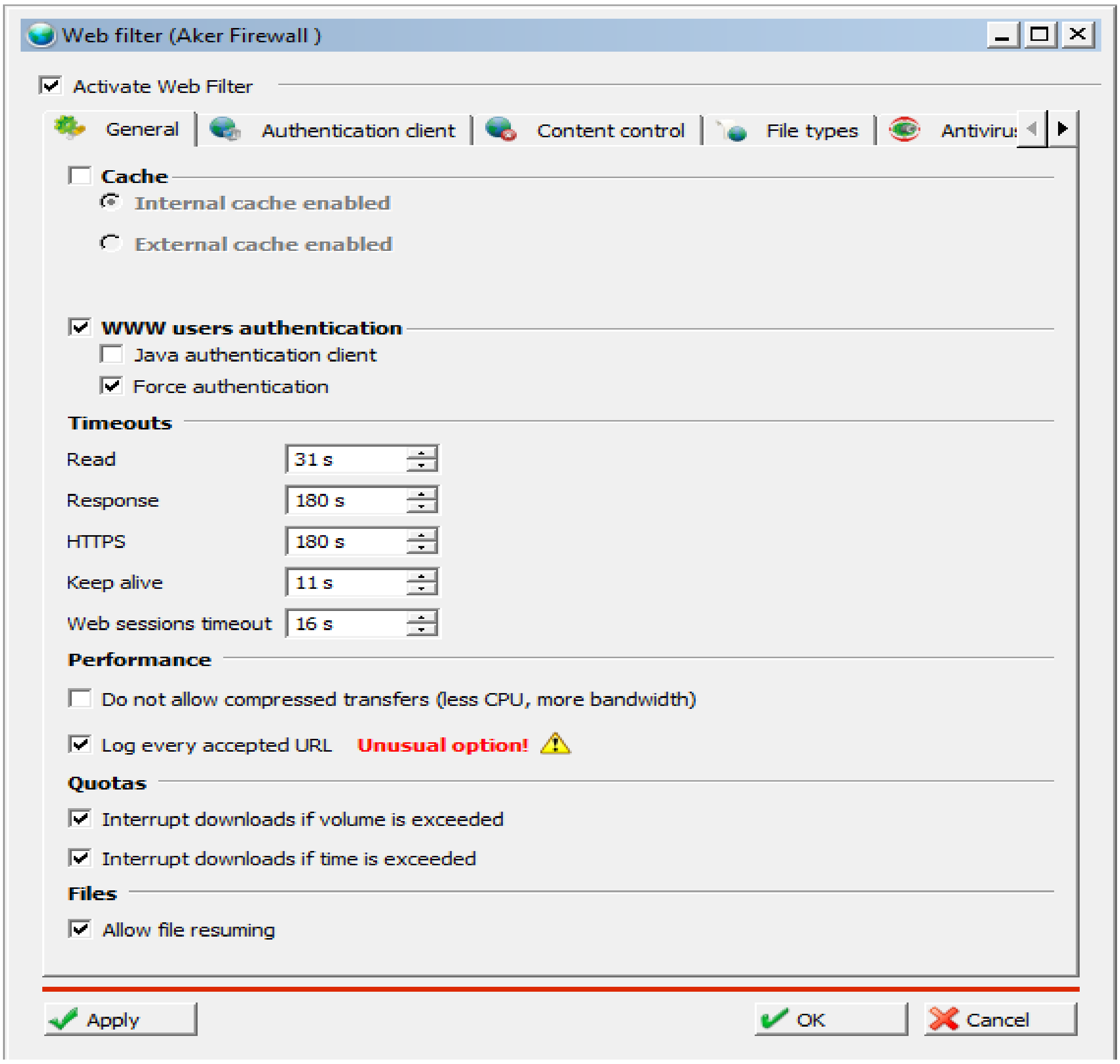

Remote Devices
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
System configurations
TCP/IP
Tools
Secure Mail Gateway - 2.2

Image 447 – Access window: web filter.

- Click on the *Application* menu
- Select *Web Filter.*

Web Filter configuration parameters

General tab



☑ Activate Web Filter

☐ **Cache**
● Internal cache enabled
○ External cache enabled

☑ **WWW users authentication**
☐ Java authentication client
☑ Force authentication

Timeouts
Read: 31 s
Response: 180 s
HTTPS: 180 s
Keep alive: 11 s
Web sessions timeout: 16 s

Performance
☐ Do not allow compressed transfers (less CPU, more bandwidth)
☑ Log every accepted URL **Unusual option!** ⚠

Quotas
☑ Interrupt downloads if volume is exceeded
☑ Interrupt downloads if time is exceeded

Files
☑ Allow file resuming

Image 448 – Web filter – general tab).

- The **OK** button will close the window saving the changes.
- The **Apply** button will save all changes and remain the window opened.
- The **Cancel** button will discard all changes closing the window.

- **Cache**

Internal cache enabled: This option allows the firewall to work as a cache server.

External cache enabled: This option defines if the Web Filter will redirect its requests to a cache server. In case this option is enabled, all received requests will be passed to the cache server, at the specified address and port. Otherwise the Web Filter will answer all requests.

IP: This field specifies the cache server IP address where the requests will be redirected, if the option *cache enabled* is active.

Port: This field specifies the port which the cache server expects to receive the connections, if the option *cache enabled* is active.

- **Parameters**

This tab adjusts the Web Filter operation in specifics situation. It consists of the following fields:

WWW users authentication: This field activate or not the Web Filter user authentication. If this option is checked, identification and password will be requested from user every time he attempts to start a session, and this session will be started only if this user be authenticated by one of the authenticators.

Java authentication client: This option instructs the proxy to use the authentication client in Java, even operating in non-transparent mode. This client advantage is that it allows the complete user authentication (as when the authentication client is used for Windows, and not only for Web Filter).

In oder to make the Java authentication client work in your browser, the browser must have Java support installed and enabled, besides allowing the UDP protocol use for Java applets.

Force authentication: If this option is checked the proxy will force the user authentication, i.e. only authenticated users will have access. If unchecked and a user wishes to authenticated, he can do it but *not identified access* will be granted.

For authentication clients who are using the HTTP1.1 protocol, it is required to disable the Java authentication, and configure the proxy-active mode.

- **Timeouts**

Read: Defines the maximum time in second that the proxy waits for a client request, as soon as a new connection is established. If the limit time has been reached, and the client has not made any request the connection will be cancelled.

Response: Defines the maximum time in second that the proxy waits for an answer of a request sent to WWW (World Wide Web) remote server or to the cache server, in case the option *enabled cache* is active. If the limit time has been reached, and the server has not started to transmit an answer, the connection with the server will be canceled and the client will receive an error message.

HTTPS: Defines the maximum time in second that the proxy can stay without receive data from the client or server in a HTTPS connection, without it considering the connection inactive and cancel it.

Keep alive: Defines the time that a user can keep a connection keep-alive (HTTP 1.) with the inactive proxy, before the proxy close it, releasing the process to other user. It is recommended to keep this time very low, to avoid the unnecessary user of all system process.

Web session timeout: Indicates the time that the web session will be monitored, allowing the administrator know which web sessions have been activated on your firewall.

Example: In case you select 30 seconds in this field, the web session (information-> Web session) will show only the active sessions from the last 30 seconds.

- **Performance**

Do not allow compressed transfers (less CPU, more bandwidth): Allows the firewall to do not accept web filter transfer containing compacted data.

In a HTTP or HTTPS request can be specified that the data comes compacted. In case the data comes compressed and there is Active-X, Java our JavaScript compressed, the firewall needs to unzip them to analyze the data.

Log every accepted URL: Allows the firewall logs all URLs that are performed in method (GET, POST and etc.), this way we shall have a larger volume of log for the report generation and Quotas accounting.

For a greater performance and resource management, the Web Filter process is created automatically by the firewall, according to the requests.

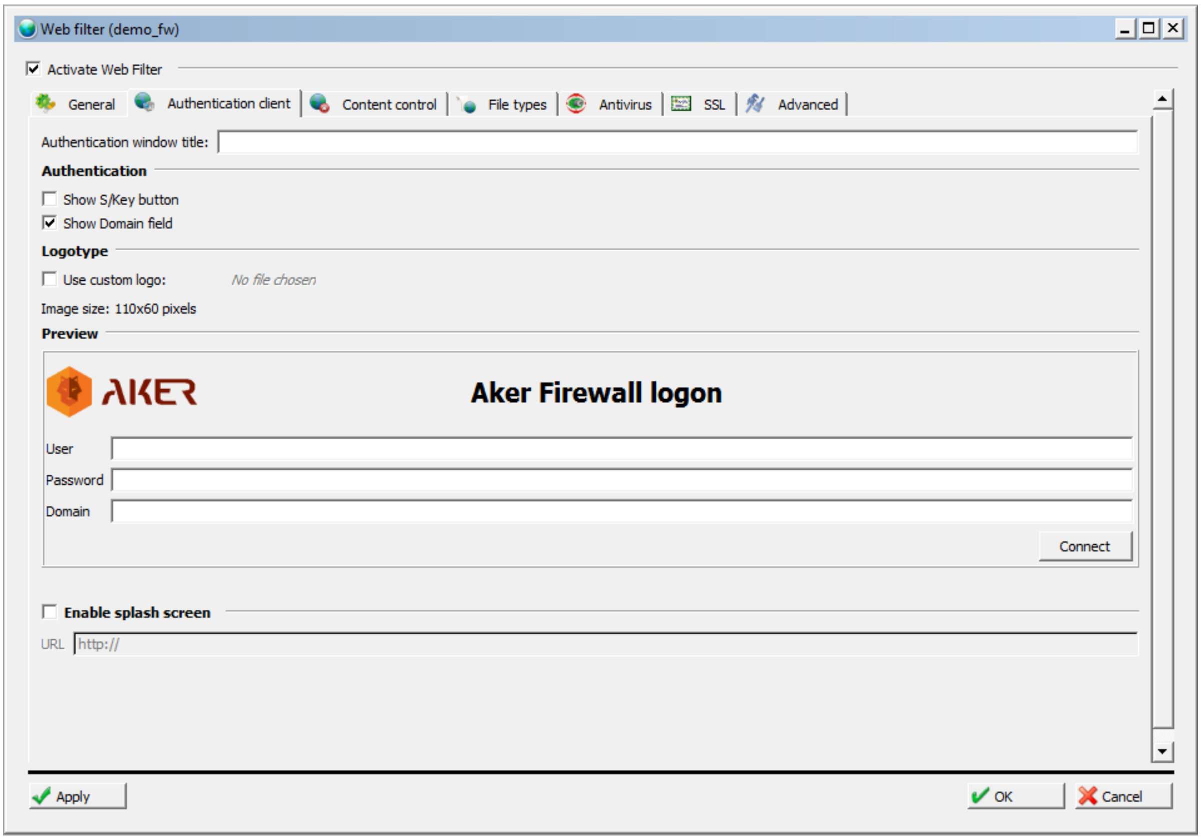
- **Quotas**

Interrupt downloads if volume is exceeded: This option allows the file transfer interruption in case the quota has been exceeded. If this option is not checked the firewall the firewall will verify the user’s quota before he begins to download.

- **Files**

  Allow file resuming: This option should be selected in case the user wants to continue a download from the point where it was stopped.

Authentication client tab


Web filter (demo_fw)
General
Authentication client
Content control
File types
Antivirus
SSL
Advanced
Authentication window title:
Authentication
Logotype
Preview
Aker Firewall logon
User
Password
Domain
Connect
URL
http://
Apply
OK
Cancel

☑ Activate Web Filter

☐ Show S/Key button

☑ Show Domain field

☐ Use custom logo: No file chosen

Image size: 110x60 pixels

☐ Enable splash screen

Image 449 – Web filter: Authentication client.

This tab is used to arrange Aker Firewall authentication window Layout.

- Create a title for the authentication window.

Authentication – This field has two options that will be available for the firewall user; this user can be connected enabling the following options:

- **Show S/Key button** – Allows the users to authenticate themselves using S/Key.
- **Show Domain field** – The user shall inform the domain to login the Web Filter.

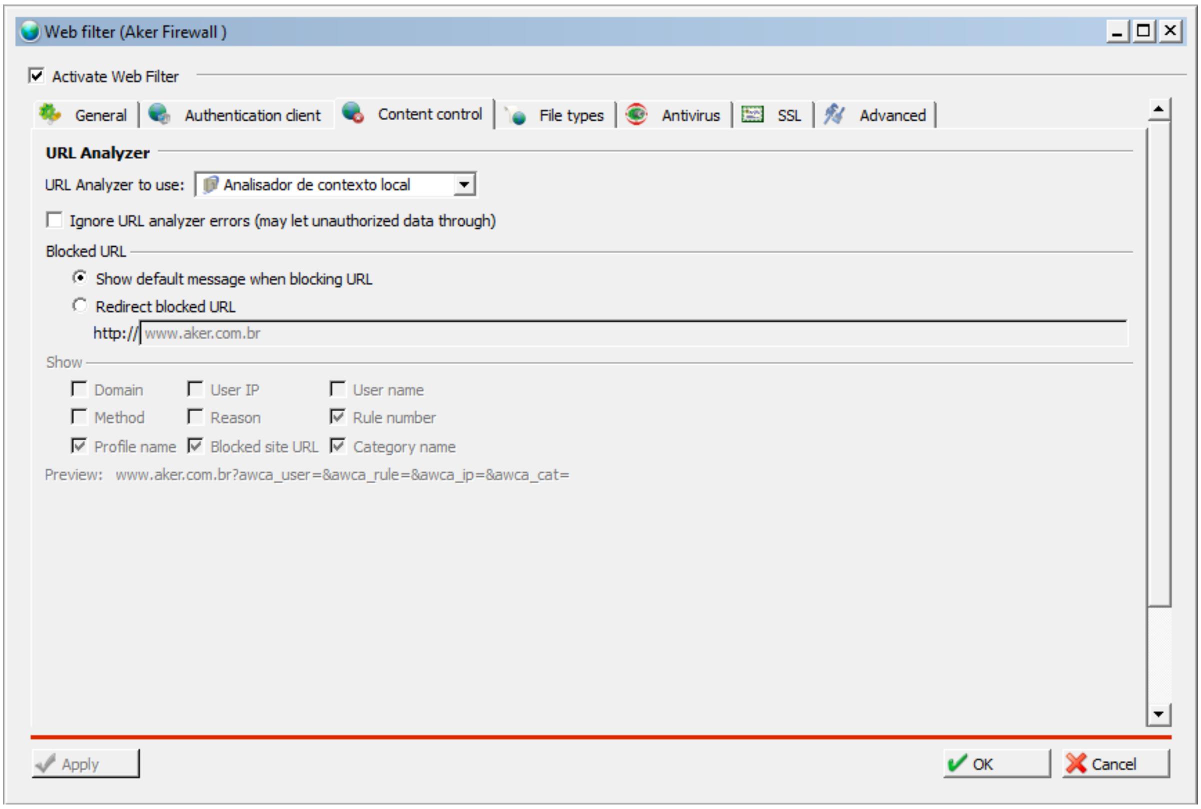
Logotype

- Use custom logo, selecting this option you will be requested to inform the logotype location in your computer.

In the **Preview** area you will be able to follow the logotype changes.

Enable splash screen: This option displays a window with the specified URL before requesting the user authentication through **Java authentication client.**

Content Control tab



☑ Activate Web Filter

URL Analyzer

URL Analyzer to use: Analisador de contexto local

☐ Ignore URL analyzer errors (may let unauthorized data through)

Blocked URL

● Show default message when blocking URL

○ Redirect blocked URL

http:// www.aker.com.br

Show

☐ Domain ☐ User IP ☐ User name
☐ Method ☐ Reason ☑ Rule number
☑ Profile name ☑ Blocked site URL ☑ Category name

Preview: www.aker.com.br?awca_user=&awca_rule=&awca_ip=&awca_cat=

Image 450 – Web Filter: content control.

URL Analyzer: Specifies the URL Analyzer that will be used to classify the Internet pages. This agent needs to be previously registered in the firewall. For more information see the chapter titled Registering entities.

Blocked URL: Configures the action taken by the firewall when a user attempt to access a blocked URL, this option consists of the following options:

- **Show default message when blocking URL**: Selecting this option the firewall shows an error message informing the selected URL has been blocked.
- **Redirect blocked URL**: Selecting this option, the firewall will redirect all *Blocked URLs access attempts* to a URL selected by the administrator. In this case the user needs to specify the URL which the blocked access will be redirected without http:// prefix.

Show: This option defines the page that will be displayed to user when attempting to access a URL is blocked. So users have two options; the default page or redirect to a selected page which will be customized according to the selected checkboxes.

Each of these checkboxes is parameters, and they are used to identify where and why the page has been blocked.

Domain: When this option is selected the URL domain will be displayed. Example: At URL www.aker.com.br, the domain would be **aker.com.br**. When the domain is selected the *domain variable* will be created.

Method: Informs the method used by the HTTP protocol. E.g. GET, PUT, POST. When the method is selected the *method variable* will be created.

Profile name: Name given by user to the selected profile. When this option is selected the *variable profile* will be created.

User IP: User's IP address who has attempted to access the blocked URL. When this option is selected the *IP variable* will be created.

Reason: When this option is selected the *variable Reason* will be created.
Enabling this option the reason of the website blocking will be displayed.
Bellow follows examples of reasons:

"URL category",
"Rule block",
"exceeded quota bytes",
"insufficient quota bytes "
"exceeded quota time",
"object type not allowed",
"file type not allowed globally",
"file type not allowed in the profile",
"connect for specified port not allowed"

Category name: Category name that was associated to the URL. When this option is selected the *cats variable* will be created.

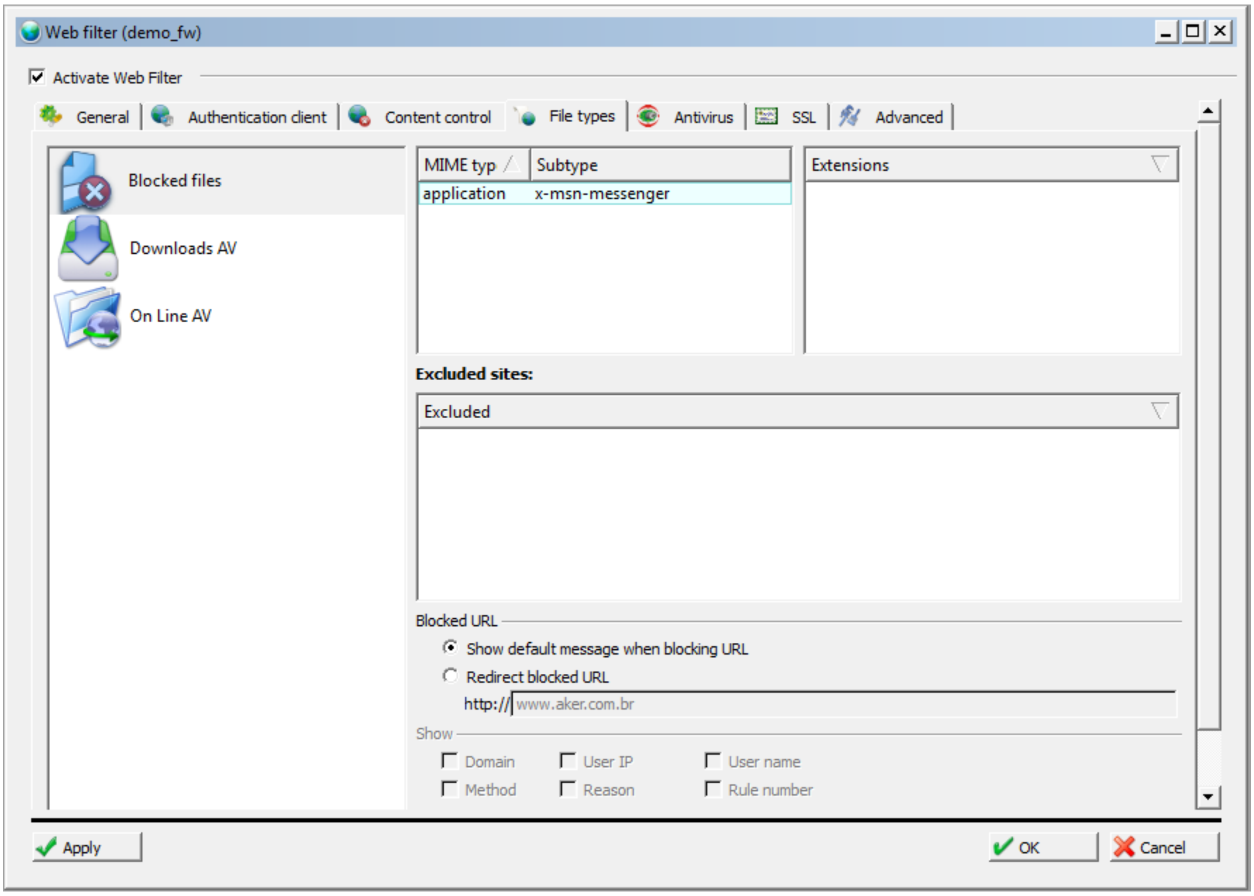
User name: User name who has attempted to access the URL. When this option is selected the *user variable* will be created

Rule number: Filtering rule number that the URL has fit. When this option is selected the *rule variable* will be created.

Blocked site URL: Shows the URL that the user has attempted to access and was blocked. When this option is selected the *URL variable* will be created.

Preview shows the URL and what will be sent via GET method.

File types tab


Web filter (demo_fw)
General
Authentication client
Content control
File types
Antivirus
SSL
Advanced
Blocked files
Downloads AV
On Line AV
Apply
OK
Cancel

☑ Activate Web Filter

MIME typ	Subtype
application	x-msn-messenger

Extensions

Excluded sites:

Excluded

Blocked URL

● Show default message when blocking URL

○ Redirect blocked URL

http:// www.aker.com.br

Show

☐ Domain ☐ User IP ☐ User name

☐ Method ☐ Reason ☐ Rule number

Image 451 – Web Filter; File types.

Blocked files

This tab specifies the files that the profile and the Web Filter will block.

In order to decide if a transferred file needs to be blocked, you may use one of the following options: the file extension or its MIME type. If one of these options is met, the firewall will block this file.

The MIME type consists of two identifiers, the first one indicates the type and the second indicates the subtype. The browser uses this information to decide how to show the received information in the same manner that the operating system uses the file extension name.

Blocked URL: Configures the action taken by the firewall when a user attempt to access a blocked URL, this option consists of the following options:

- **Show default message when blocking URL**: Selecting this option the firewall shows an error message informing the selected URL has been blocked.
- **Redirect blocked URL**: Selecting this option, the firewall will redirect all *Blocked URLs access attempts* to a URL selected by the administrator. In this case the user needs to specify the URL which the blocked access will be redirected without http:// prefix.

Show: This option defines the page that will be displayed to user when attempting to access a URL is blocked. So users have two options; the default page or redirect to a selected page which will be customized according to the selected checkboxes.

Each of these checkboxes is parameters, and they are used to identify where and why the page has been blocked.

Domain: When this option is selected the URL domain will be displayed. Example: At URL www.aker.com.br, the domain would be **aker.com.br**. When the domain is selected the *domain variable* will be created.

Method: Informs the method used by the HTTP protocol. E.g. GET, PUT, POST. When the method is selected the *method variable* will be created.

Profile name: Name given by user to the selected profile. When this option is selected the *variable profile* will be created.

User IP: User's IP address who has attempted to access the blocked URL. When this option is selected the *IP variable* will be created.

Reason: When this option is selected the *variable Reason* will be created.
Enabling this option the reason of the website blocking will be displayed.
Bellow follows examples of reasons:

"URL category",
"Rule block",
"exceeded quota bytes",
"insufficient quota bytes "
"exceeded quota time",
"object type not allowed",
"file type not allowed globally",
"file type not allowed in the profile",
"connect for specified port not allowed"

Category name: Category name that was associated to the URL. When this option is selected the *cats variable* will be created.

User name: User name who has attempted to access the URL. When this option is selected the *user variable* will be created

Rule number: Filtering rule number that the URL has fit. When this option is selected the *rule variable* will be created.

Blocked site URL: Shows the URL that the user has attempted to access and was blocked. When this option is selected the *URL variable* will be created.

Preview shows the URL and what will be sent via GET method.

.

Downloads

Specify the files that will be analyzed against virus by *Aker Firewall Download manager*. This option is interesting for large files (zipped files as example) or files that normally are not viewable on-line through the browser.

In order to decide if a transferred file needs to be blocked, you may use one of the following options: the file extension or its MIME type. If one of these options is met, the firewall will block this file.

The MIME type consists of two identifiers, the first one indicates the type and the second indicates the subtype. The browser uses this information to decide how to show the received information in the same manner that the operating system uses the file extension name.

Deleted websites:

Here you need to choose the operation and the text you are including for the analysis. Web sites that fit in the deleted list will not be analyzed.

Operation menu:

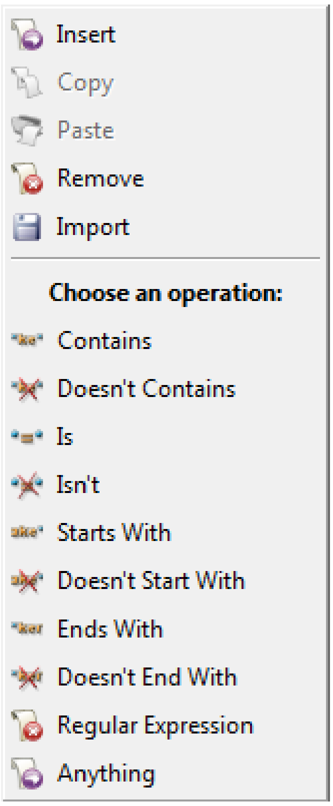

Insert
Copy
Paste
Remove
Import
Choose an operation:
Contains
Doesn't Contains
Is
Isn't
Starts With
Doesn't Start With
Ends With
Doesn't End With
Regular Expression
Anything

Image 452 – Choosing an operation.

Configurations:

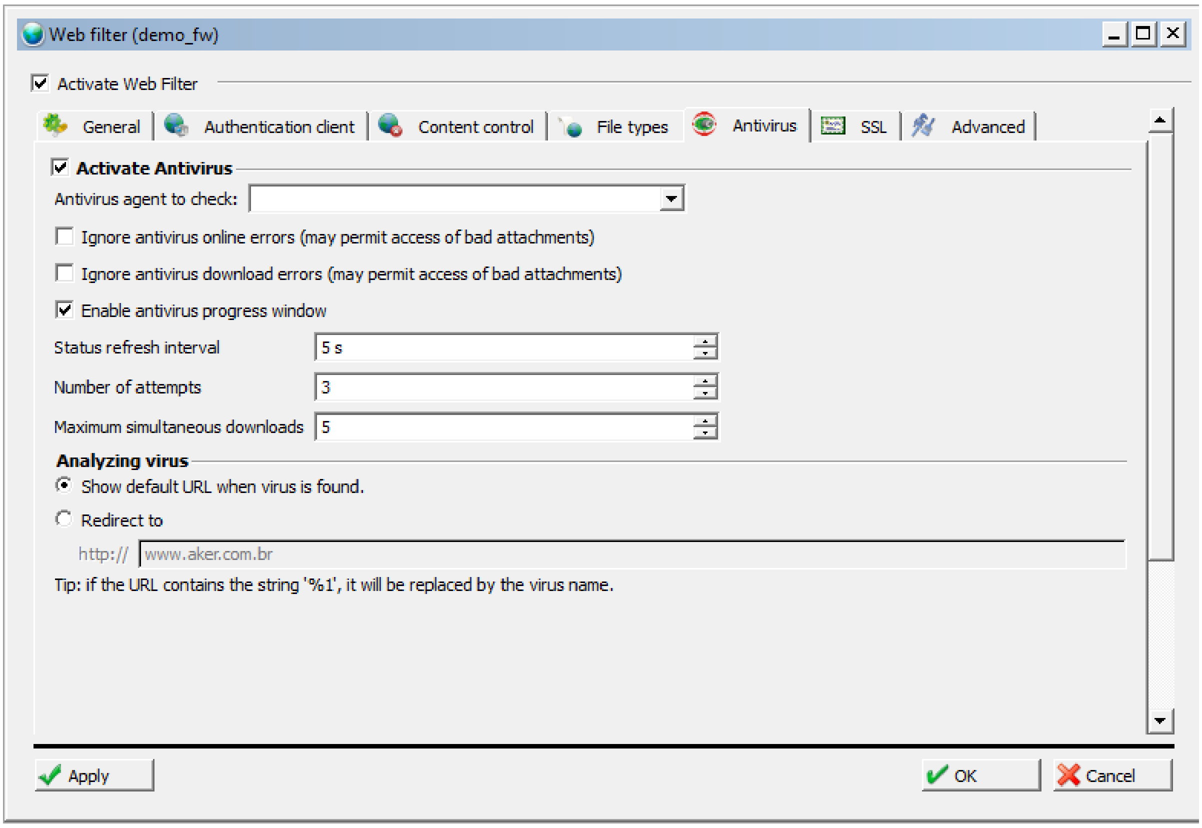
Encrypted files: You choose between accept or reject an encrypted attachment.

Corrupted files: You choose between accept or reject a corrupted attachment.

Online

Same as the download option, the firewall administrator shall choose the MIME types and the extensions.

Aba Antivirus



☑ Activate Web Filter

☑ **Activate Antivirus**

Antivirus agent to check:

☐ Ignore antivirus online errors (may permit access of bad attachments)

☐ Ignore antivirus download errors (may permit access of bad attachments)

☑ Enable antivirus progress window

Status refresh interval: 5 s

Number of attempts: 3

Maximum simultaneous downloads: 5

Analyzing virus

● Show default URL when virus is found.

○ Redirect to

http:// www.aker.com.br

Tip: if the URL contains the string '%1', it will be replaced by the virus name.

Image 453 – Web Filter: antivirus.

Activate Antivirus: Selecting this option, the firewall will be allowed to perform an antivirus verification of contents that have been downloaded.

The Reset to defaults button restores the firewall original configuration for this tab.

- **Antivirus agent to check:** Chooses an antivirus agent previously registered to perform the virus verification. For more information see the chapter tittled **Registering entities**.
- **Ignore antivirus online errors (may permit access of bad attachments)** In case this option is selected, and there is an analysis error on the on-line traffic, the traffic will not be blocked, allowing the data transfer. If this option is not selected the data transfer will be blocked.
- **Ignore antivirus download errors (may permit access of bad attachments**: In case this option is selected, and there is an analysis error on the on-line traffic, it will not block the download, allowing the data transfer. If this option is not selected the download will be blocked.
- **Enable antivirus progress window:** This option allows disabling the *Aker Firewall Download manager*.
- **Status refresh interval:** This option specifies the amount of time that the download page displayed by the firewall will be refreshed.

- **Number of attempts:** Maximum number of downloads attempts for each files, in case it is necessary to attempt to download the file more than one time.
- **Maximum simultaneous downloads:** Configures the maximum number of simultaneous downloads allowed by the firewall.

Analyzing virus: This option shows a page in case a virus is found during the antivirus analysis. This page can be the firewall page or a page customized by the user, and you also can custom a message for each type of virus detected, simply using the string {VIR} that will be replaced by the virus name.

- **Show default URL when virus is found**: Selecting this option the firewall shows an error message informing the selected URL has been blocked.
- **Redirect to**: Selecting this option, the firewall will redirect all *Blocked URLs access attempts* to a URL selected by the administrator. In this case the user needs to specify the URL which the blocked access will be redirected without http:// prefix.

Web Filter -SSL

HTTPS proxy is the Web Filter part that deals with TCP connections through port 443. The principle of operation is the one of a *man-in-the-middle attack:* the host client access through Aker Firewall, and Aker Firewall with the remote server in a transparent way.

Learning a bit about certificates

What is a digital certificate?

Digital certificate is a document provided by the certified entity for each entity that will perform a communication, the digital certificate purpose is guarantee the authenticity.

For certificates used in the HTTPS communication the default is X.509. It normally uses the extensions “pem”, “cer” and “crt”.

PKCS#12 format

The PKCS#12 format was created by “RSA Laboratories” to store the X.509 certificate followed by the private key. This file normally has the “pfx” and “p12” extension.

HTTPS communication

The HTTPS communication uses the digital certificate system.

When client accesses a website with HTTPS the server sends to client the X.509 certificate that contains his private key.

With the certificate on hands the client does some validations:

- Verify the certificate’s Validity;
- Verify the URL host and the certificate’s Common Name (CN).
- Verify if the certified authority which signed the certificate is a trusted authority.

Successfully authenticated the client performs the communication process of HTTP requests and response.

See the diagram below:

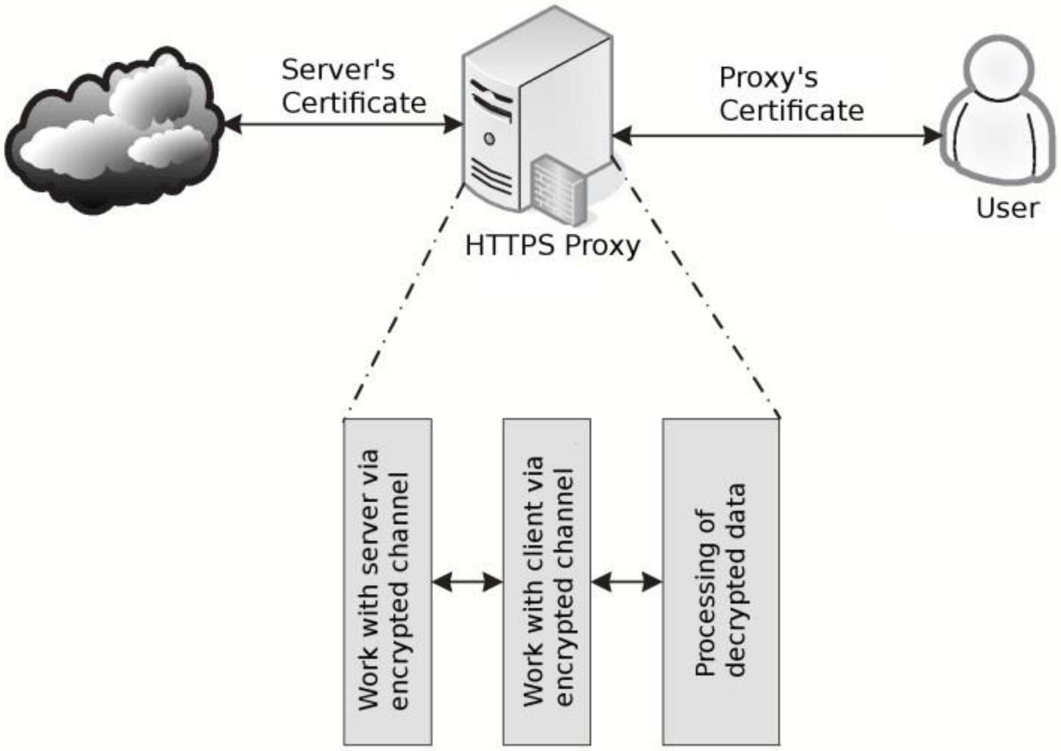

Server's Certificate
Proxy's Certificate
User
HTTPS Proxy
Work with server via encrypted channel
Work with client via encrypted channel
Processing of decrypted data

Image 454 – Certificate diagram.

The diagram shows the certificates involved in the access:

- **Remote server certificate:** original certificate where data with expiration date and common name are copied to certificates generated in the firewall.
- **Proxy certificate:** certificate created for each request that has the copy of the original certificate data that identify the website, signed by CA inserted by the administrator

The clients need trust in this CA inserted in Aker Firewall, so your browser does not detect the attack. After, two certificates are required; one to clients and the other to Aker Firewall.

Other certificates presented are used by Aker Firewall to validate remote websites.

Generating a certificate for Firewall usage.

To generate certificates the firewall needs to act as a Certificate authority (CA), i.e. it generates the certificates to websites which are accessed through proxy. To perform this process few prerequisites are required:

- The firewall needs a PKCS#12 digital certificate, because only this one has the private key;
- The X.509 contained in the PKCS#12 needs to be a certificate with prerogatives so this certificate will be able to sign new certificates, i.e. it acts as a CA.

There are many possibilities for the certificate generation process, in this FAQ there will be two options.

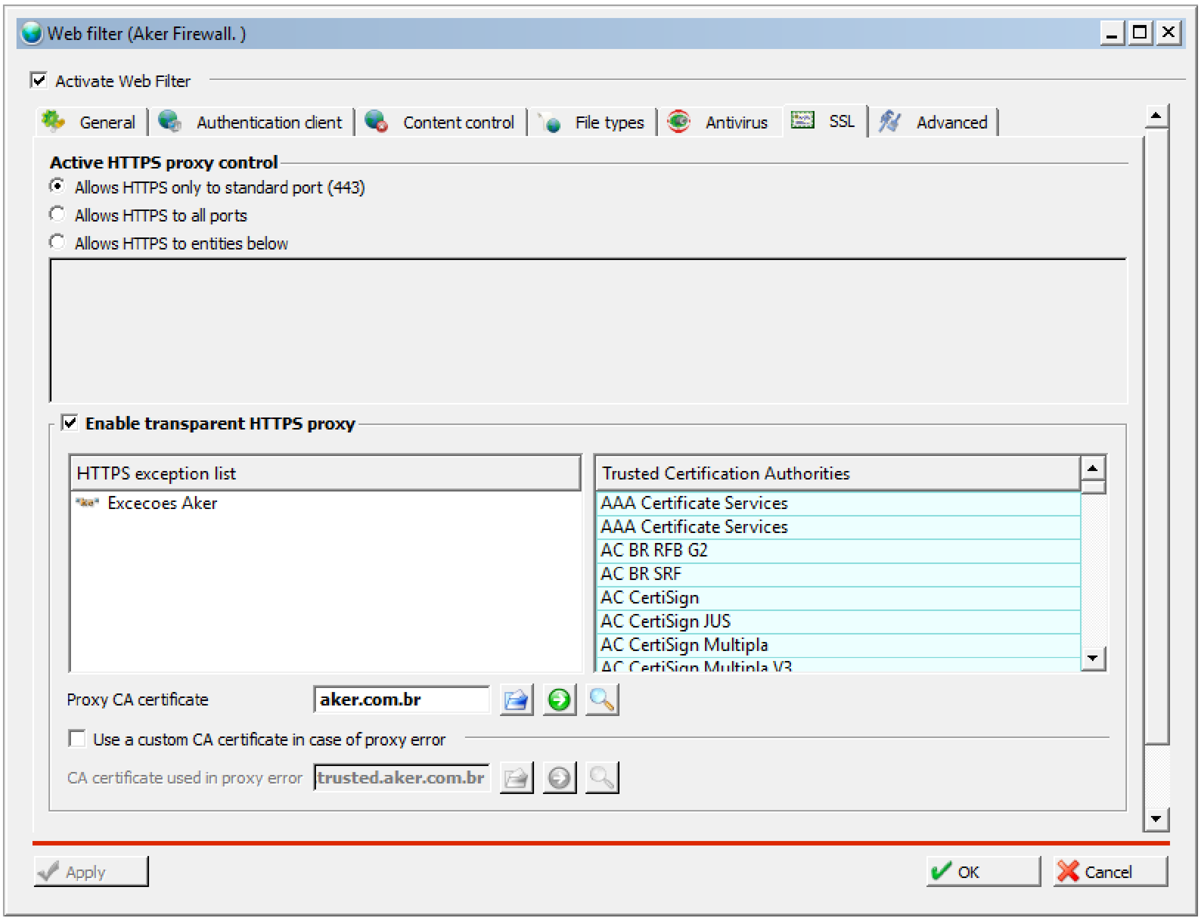
1. Generate a self-signed certificate with the OpenSSL;
2. Use a certificate of a Windows root certificate authority.

At the end of each of the processes above, there will be two files that will be used in the proxy HTTPS process:

1. X.509 file with **.cer** extension;
2. PKCS#12 file with **.pfx.** extension;

The PKCS#12 file will be used in the HTTPS proxy configuration and the X.509 file needs to be imported in the **trusted root certification authorities.**

SSL tab



☑ Activate Web Filter

Active HTTPS proxy control

● Allows HTTPS only to standard port (443)

○ Allows HTTPS to all ports

○ Allows HTTPS to entities below

☑ **Enable transparent HTTPS proxy**

HTTPS exception list	Trusted Certification Authorities
Excecoes Aker	AAA Certificate Services
	AAA Certificate Services
	AC BR RFB G2
	AC BR SRF
	AC CertiSign
	AC CertiSign JUS
	AC CertiSign Multipla
	AC CertiSign Multipla V3

Proxy CA certificate: aker.com.br

☐ Use a custom CA certificate in case of proxy error

CA certificate used in proxy error: trusted.aker.com.br

Image 455 – Web Filter: SSL tab.

The active HTTPS proxy is will be enabled as default, and it has the filtering option for specific ports and entities.

Active HTTPS proxy control: Defines the HTTPS secure connections ports that will be accepted by the firewall. If a client attempt to open a connection to a port not permitted, the firewall will show a message of error and will deny the access.

Allows HTTPS only to standard port (443): In case you wish to use only the default port (443), this option should be chosen. This configuration is normally used in most of the firewalls.

- **Allow HTTPS to all ports:** Indicates to the firewall that it must accept HTTPS connections to any port. This configuration is not recommended to any environment that needs a reasonable security level, since it is possible to a user uses a proxy to access not permitted services simulating a HTTPS connection.
- **Allows HTTPS to entities below:** This option allows the administrator to define which ports will be permitted. In this case entities corresponding to

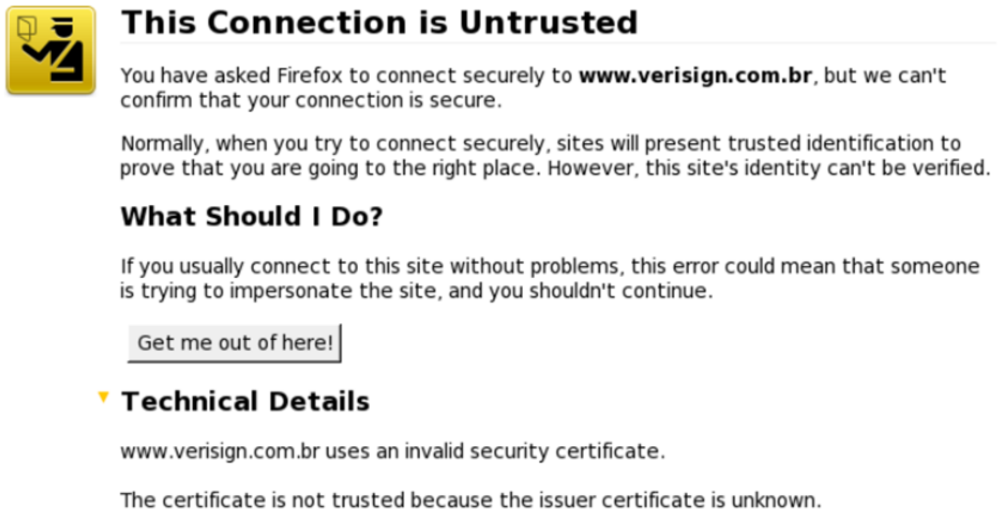
the desired services must to be registered. For more information see the chapter titled **Registering Entities**.

- **Enable transparent HTTPS Proxy**

Enabling transparent HTTPS proxy allows the creation of a filtering rule for the HTTPS service you wish to use.

- **HTTPS exception list**: In this field the entities *SSL Common Name list* that are located in the tab list on the entities widget. The website's Common Names that will not pass by the proxy need to be registered.

- **Use a custom CA certificate in case of proxy error:** In case the proxy detects that the certificate on the other side is not valid, the user need to be warned, as did the browser. If this option is not checked the access is blocked, an event will be generated and an error page will be sent to the user.



This Connection is Untrusted

You have asked Firefox to connect securely to **www.verisign.com.br**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

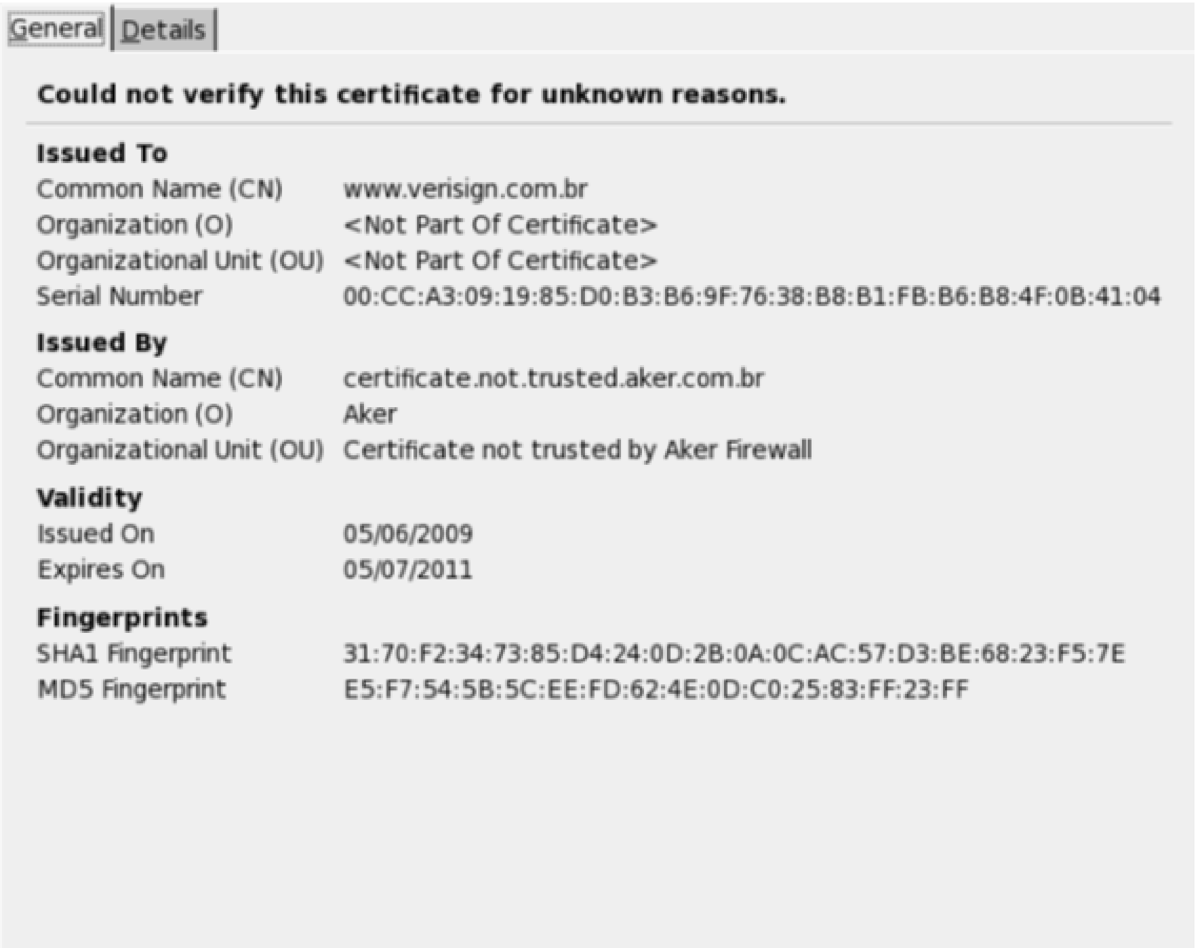
Technical Details

www.verisign.com.br uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

Image 456 – Firefox certificate error.

Firefox error when a certificate signed by CA with error is detected.



Could not verify this certificate for unknown reasons.

Issued To
Common Name (CN) www.verisign.com.br
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 00:CC:A3:09:19:85:D0:B3:B6:9F:76:38:B8:B1:FB:B6:B8:4F:0B:41:04

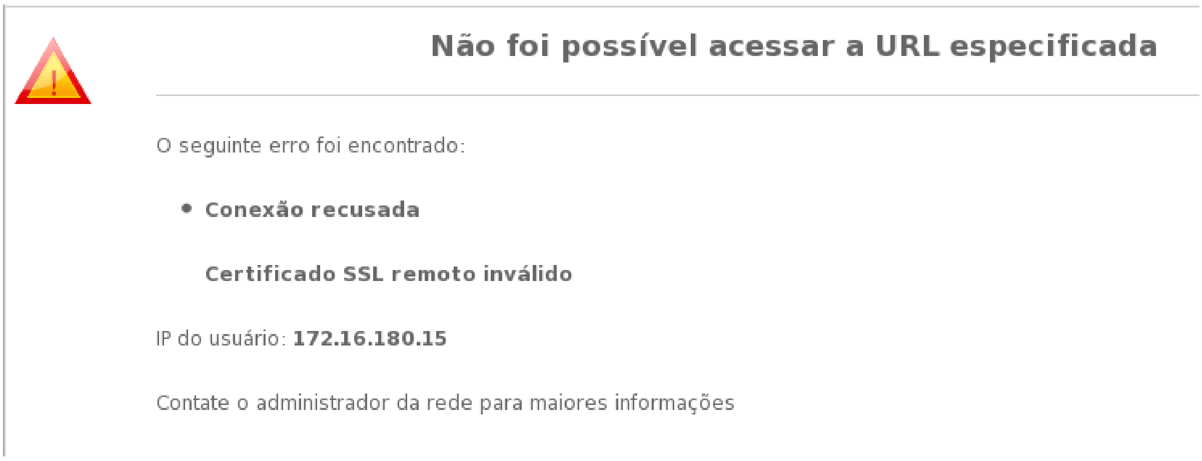
Issued By
Common Name (CN) certificate.not.trusted.aker.com.br
Organization (O) Aker
Organizational Unit (OU) Certificate not trusted by Aker Firewall

Validity
Issued On 05/06/2009
Expires On 05/07/2011

Fingerprints
SHA1 Fingerprint 31:70:F2:34:73:85:D4:24:0D:2B:0A:0C:AC:57:D3:BE:68:23:F5:7E
MD5 Fingerprint E5:F7:54:5B:5C:EE:FD:62:4E:0D:C0:25:83:FF:23:FF

Image 457 – Certificate signed by CA.

Certificate signed by CA.



Não foi possível acessar a URL especificada

O seguinte erro foi encontrado:

- **Conexão recusada**

  Certificado SSL remoto inválido

IP do usuário: **172.16.180.15**

Contate o administrador da rede para maiores informações

Image 458 – Access error.

Proxy CA certificate: In this field it is possible to *import/export* a CA used to sign the certificates.

Using the Open SSL

1. Install the OpenSSL;
2. Create a directory to be used during the process;
3. Create a file in the directory above, name this file “database.txt”;
4. Create a file in the directory above, name this file “serial.txt”;
5. Create a file named as “self-signed.conf” and add the following content:

```
RANDFILE    = .rnd

[ ca ]
default_ca  = CA_default

[ CA_default ]
certs       = certs
crl_dir           = crl
database    = database.txt
new_certs_dir     = certs
certificate = cacert.pem
serial            = serial.txt
crl         = crl.pem
private_key = private\cakey.pem
RANDFILE    = private\private.rnd
default_days      = 365
default_crl_days= 3
default_md  = sha1
preserve    = no
policy            = policy_match

[ policy_match ]
commonName        = supplied
emailAddress            = optional
countryName       = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName  = optional
organizationalUnitName  = optional

[ req ]
default_bits            = 1024
default_keyfile   = privkey.pem
distinguished_name      = req_distinguished_name

[ req_distinguished_name ]
commonName              = Common Name (eg, your website domain name)
commonName_max                = 64
emailAddress                  = Email Address
emailAddress_max        = 40
countryName             = Country Name (2 letter code)
countryName_min               = 2
countryName_max               = 2
countryName_default           = BR
```

```
stateOrProvinceName           = State or Province Name (full name)
localityName                  = Locality Name (eg, city)
0.organizationName            = Organization Name (eg, company)
organizationalUnitName        = Organizational Unit Name (eg,
section)
countryName_default           = BR

[ v3_ca ]
certificatePolicies=2.5.29.32.0
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints=critical,CA:TRUE
keyUsage = critical,cRLSign, keyCertSign, digitalSignature
```

6. Create a private key:

   ```
   openssl genrsa -des3 -out ca.key 1024
   ```

   At this moment a storage key password will be requested, this password will be used later to open the private key.

   ```
   Loading 'screen' into random state - done
   Generating RSA private key, 1024 bit long modulus
   ..............++++++
   ...............++++++
   e is 65537 (0x10001)
   Enter pass phrase for ca.key:
   ```

7. Create the X.509 certificate. This file will be used later for the client's installation:

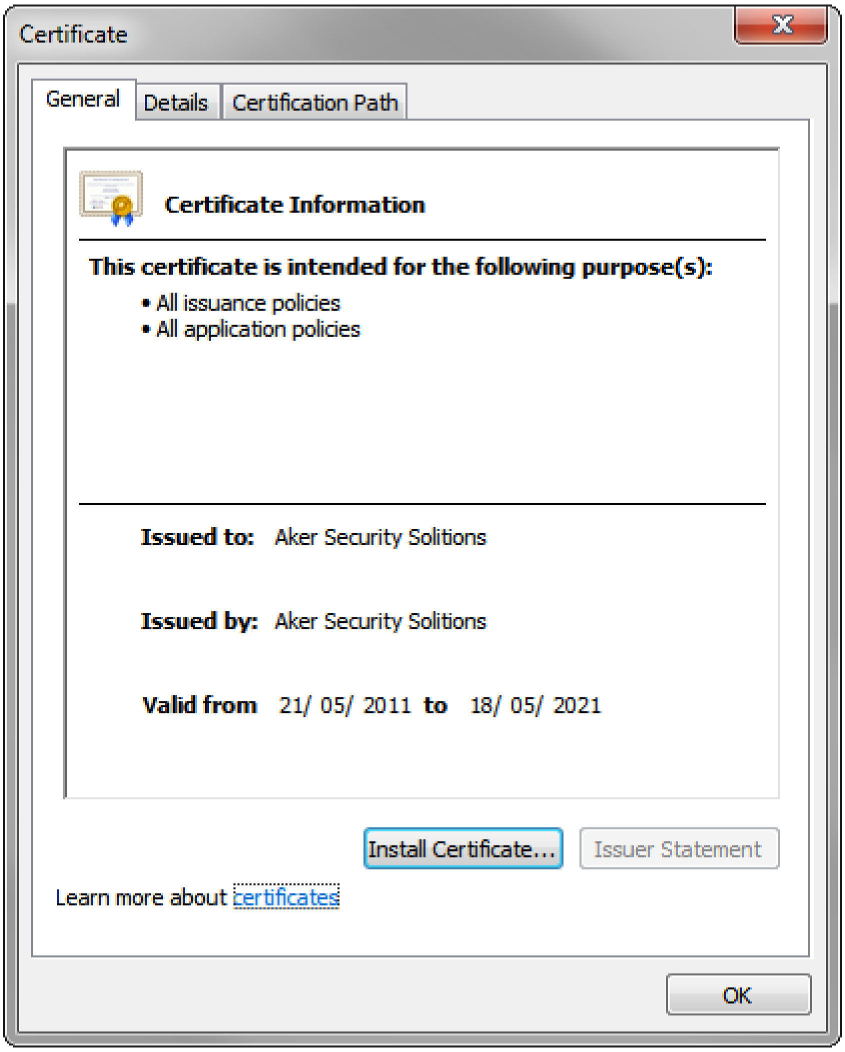
   ```
   openssl req -extensions v3_ca -config autoassinado.conf -new -x509 -
   days 3650 -key ca.key -out firewall.cer
   ```

At this moment some information will be requested, the first one of them is the private key password created above.

```
Enter pass phrase for ca.key:
```

Now the certificate data will be requested, the only mandatory item is the Common Name (CN), in it shall be added the name used to identify the CA.

Below follows Image of the certificate done through the steps above:



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Aker Security Solitions

Issued by: Aker Security Solitions

Valid from 21/ 05/ 2011 **to** 18/ 05/ 2021

Learn more about certificates

Image 459 – Certificate Information

However we have two files, one to the private key, and the other to the certificate, this way will be necessary put them in a single file in the PKCS#12 format, which is the format recognized by the firewall.

8. Create a PKCS#12 file with the private key and certificate.

```
openssl pkcs12 -export -out firewall.pfx -in firewall.cer -inkey
ca.key
```

In this process two passwords will be requested, the first one is for private key opening and the second one is to the PKCS#12 FILE EXPORT. This second password will be used when the PKCS#12 file is being imported to the firewall.

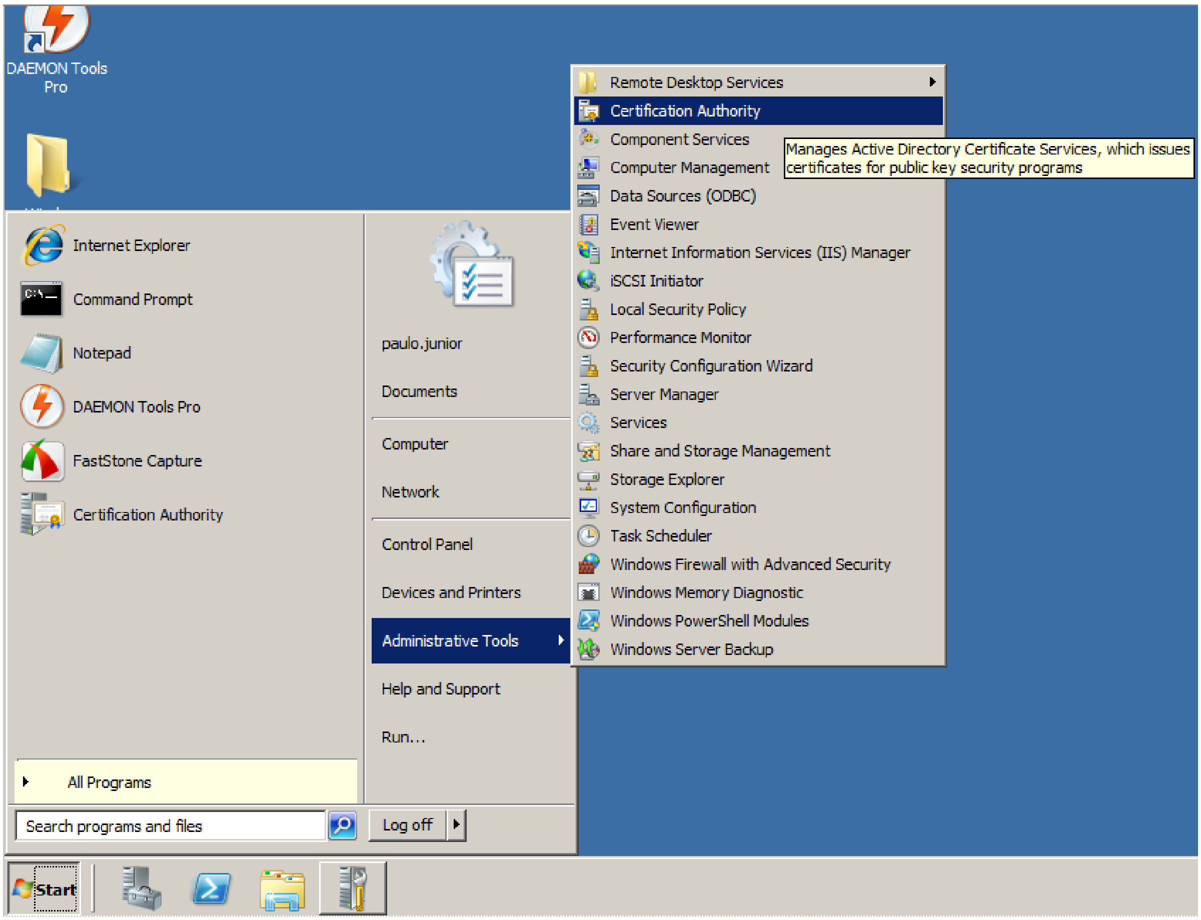
```
Enter pass phrase for ca.key:
Enter Export Password:
Verifying - Enter Export Password:
```

Using the CA Microsoft:

This item does not show how to install a certificate authority (CA) on Windows, it shows how to use one already is installed.

Below follows the instructions of how to use the CA.

1. **Start > Administrative Tools > Certification Authority**


DAEMON Tools Pro
Internet Explorer
Command Prompt
Notepad
DAEMON Tools Pro
FastStone Capture
Certification Authority
All Programs
Search programs and files
paulo.junior
Documents
Computer
Network
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Log off
Remote Desktop Services
Certification Authority
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup
Start

Manages Active Directory Certificate Services, which issues certificates for public key security programs

Image 460 – Certificate Information

2. Select your CA.

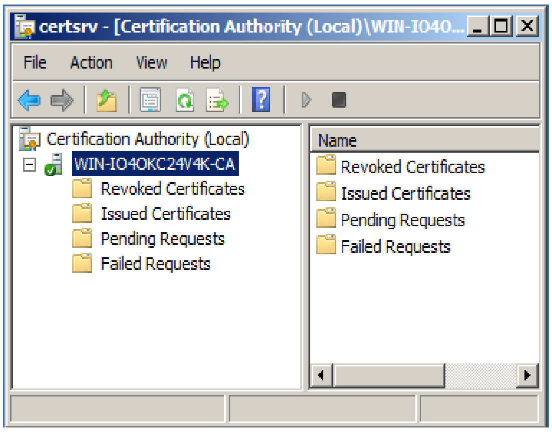

certsrv - [Certification Authority (Local)\WIN-IO40...
File
Action
View
Help
Certification Authority (Local)
WIN-IO4OKC24V4K-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Name
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests

Image 461 – Certification Authority

3. Exporting the X.509 certificate from CA.

Right-click on **Properties**

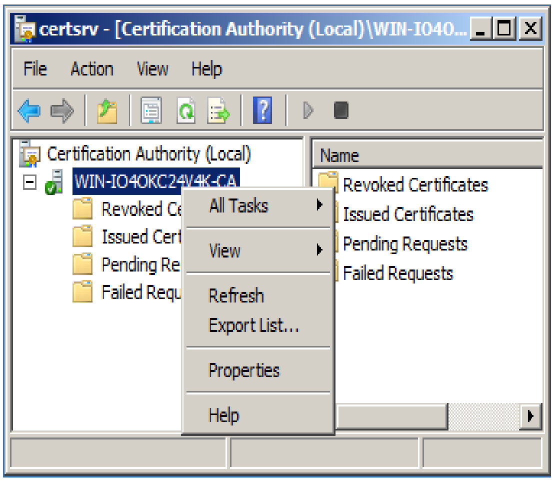
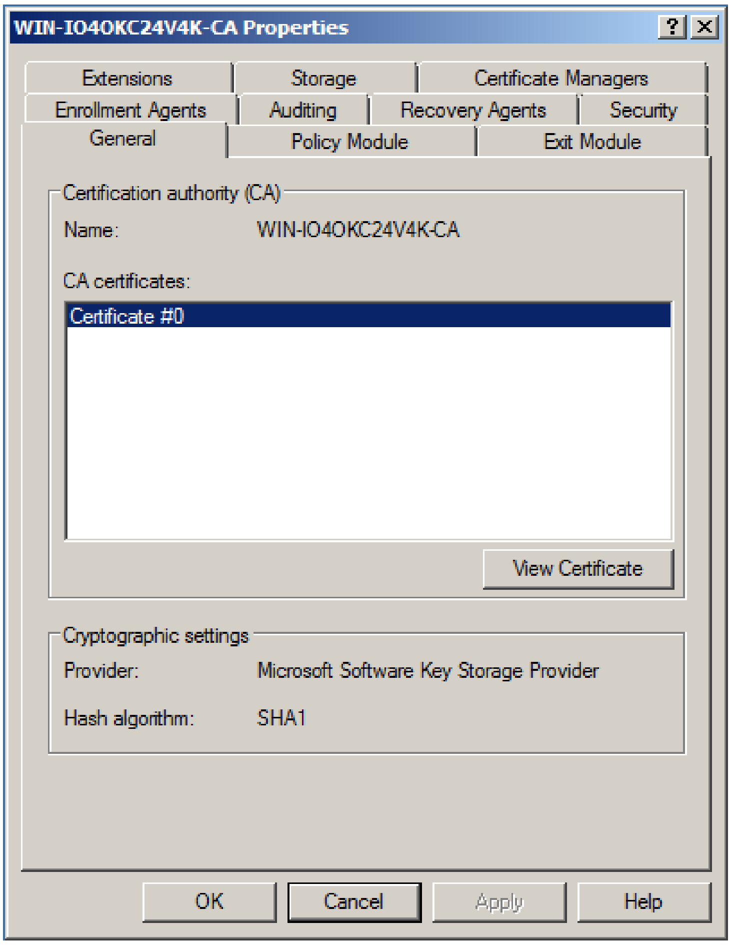

certsrv - [Certification Authority (Local)\WIN-IO40...
File
Action
View
Help
Certification Authority (Local)
WIN-IO4OKC24V4K-CA
Revoked Ce
Issued Cert
Pending Re
Failed Requ
All Tasks
View
Refresh
Export List...
Properties
Help
Name
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests

Image 462 – CA certificate – properties.

4. Select the last certificate and click on View Certificate


WIN-IO4OKC24V4K-CA Properties
?
Extensions
Storage
Certificate Managers
Enrollment Agents
Auditing
Recovery Agents
Security
General
Policy Module
Exit Module
View Certificate
OK
Cancel
Apply
Help

Certification authority (CA)

Name: WIN-IO4OKC24V4K-CA

CA certificates:

Certificate #0

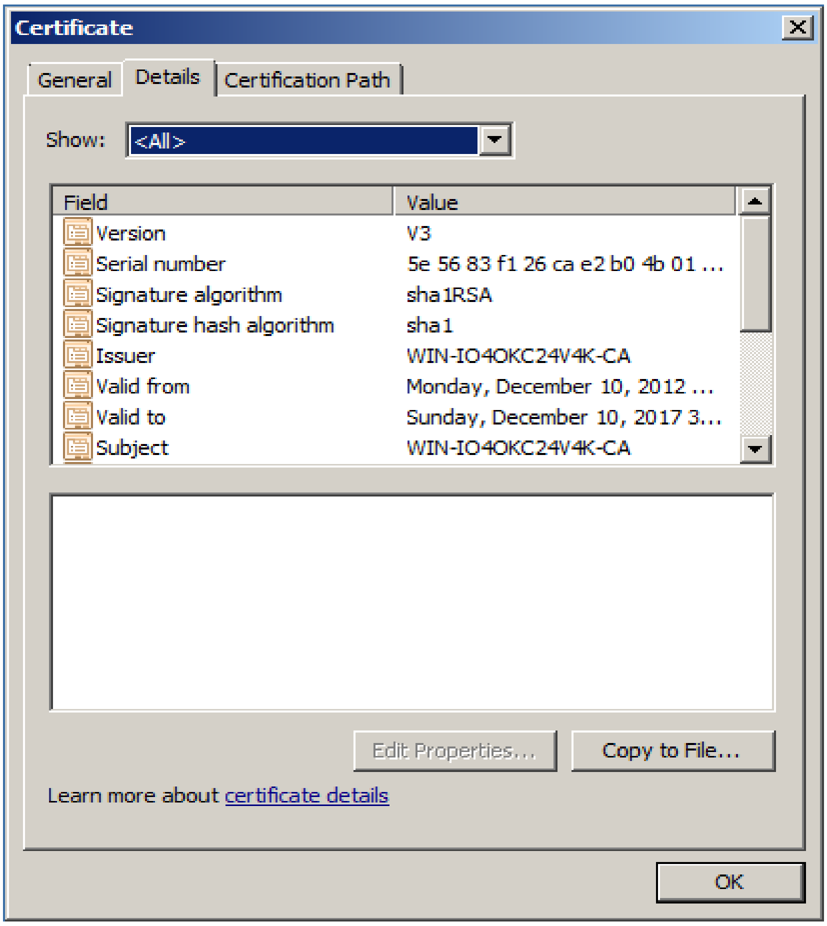
Cryptographic settings

Provider: Microsoft Software Key Storage Provider

Hash algorithm: SHA1

Image 463 – CA Certificate (General)

5. Select the **Details tab** them click on **Copy to file**



Certificate
General
Details
Certification Path
Show:
<All>
Edit Properties...
Copy to File...
Learn more about certificate details
OK

Field	Value
Version	V3
Serial number	5e 56 83 f1 26 ca e2 b0 4b 01 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	WIN-IO4OKC24V4K-CA
Valid from	Monday, December 10, 2012 ...
Valid to	Sunday, December 10, 2017 3...
Subject	WIN-IO4OKC24V4K-CA

Image 464 – CA certificate (Details)

6. Select the location to save the file (this file will be used later for clients' installation).

7. In the following steps we shall export the file in PKCS#12 format for the firewall usage.

8. Go back to the *Certification Authority* main window, and right-click on the CA's name and click on > **All Tasks** > **Back up CA**

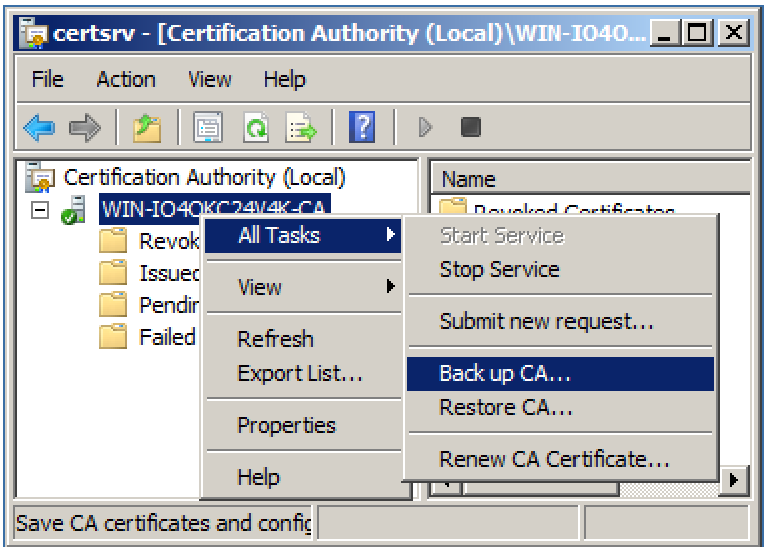
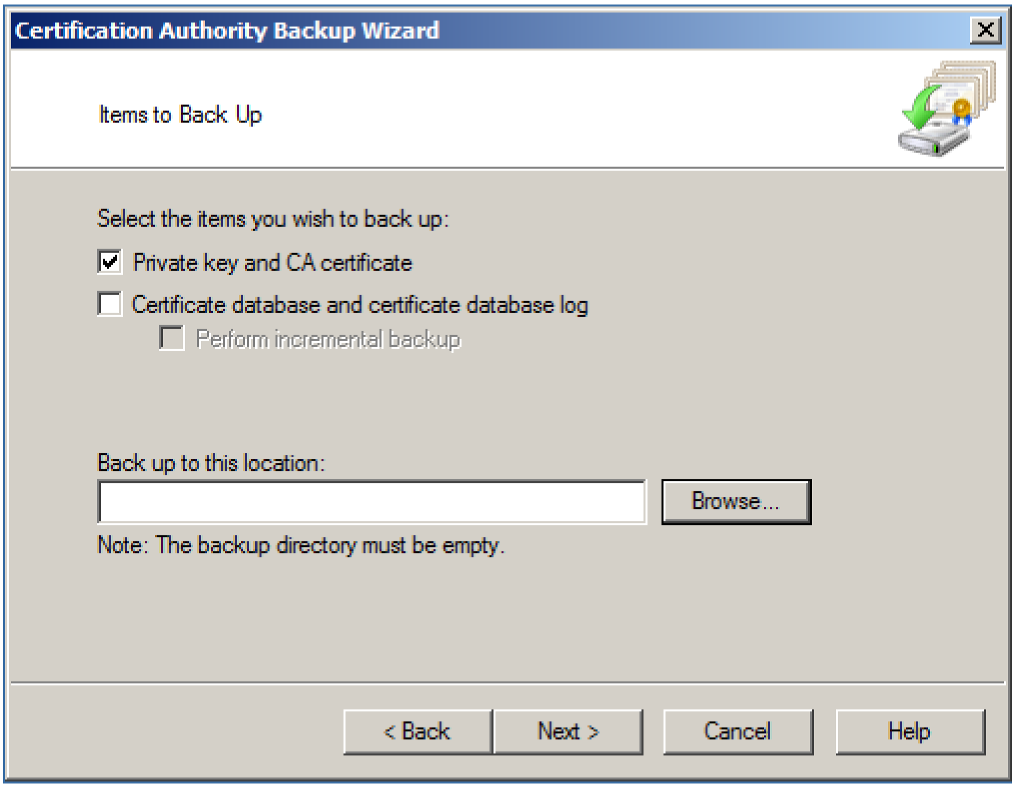

certsrv - [Certification Authority (Local)\WIN-IO40...
File
Action
View
Help
Certification Authority (Local)
WIN-IO4QKC24V4K-CA
Revok
Issuec
Pendir
Failed
Name
Revoked Certificates
All Tasks
View
Refresh
Export List...
Properties
Help
Start Service
Stop Service
Submit new request...
Back up CA...
Restore CA...
Renew CA Certificate...
Save CA certificates and confic

Image 465 – Certificate CA (All tasks / Back up Ca)

9. On the following screen click on ***Next***. Them the screen below will be displayed, select only the option **Private key and CA certificate**, indicate the directory you wish to save the file, and click **Next.**


Certification Authority Backup Wizard

Items to Back Up

Select the items you wish to back up:

☑ Private key and CA certificate

☐ Certificate database and certificate database log

☐ Perform incremental backup

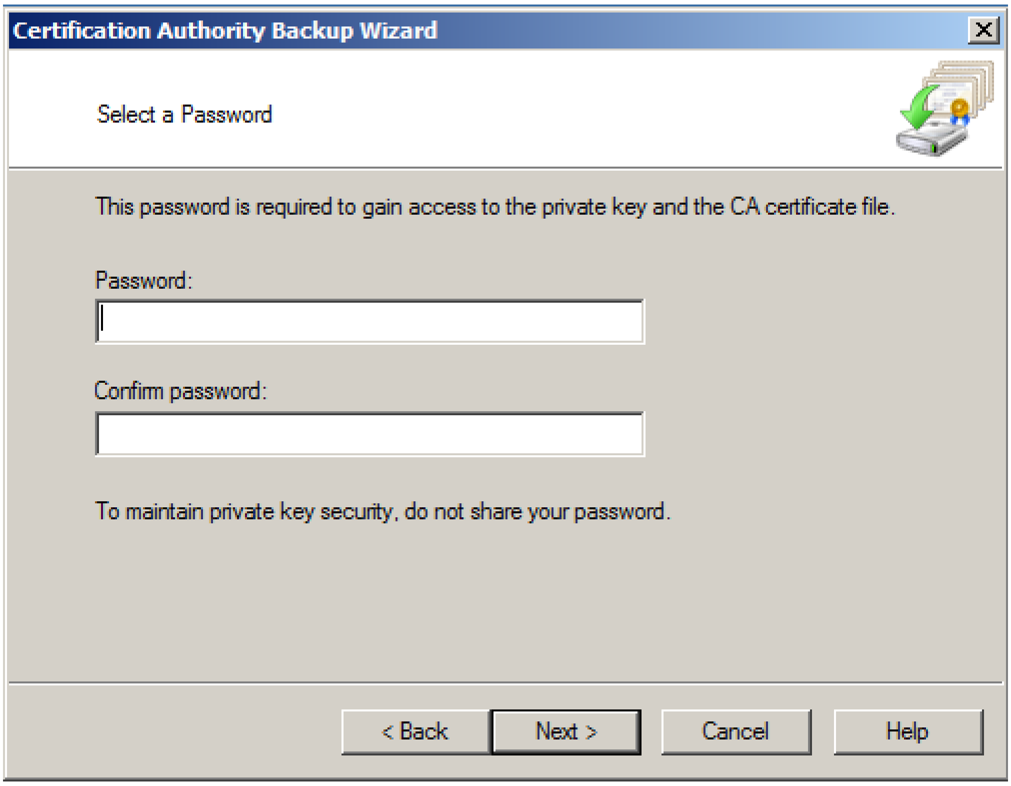
Back up to this location:

Note: The backup directory must be empty.

Browse...
< Back
Next >
Cancel
Help

Image 466 – Certification Authority Backup Wizard

10. The following screen indicates the PKCS#12 file protection password. This password will be used when the PKCS#12 file is being imported in the firewall.



This password is required to gain access to the private key and the CA certificate file.

Password:

Confirm password:

To maintain private key security, do not share your password.

Image 467 – Certification Authority Backup Wizard – Password and confirmation.

After the process above is done, a PKCS#12 file with the private key and the certificate of this CA will be created.

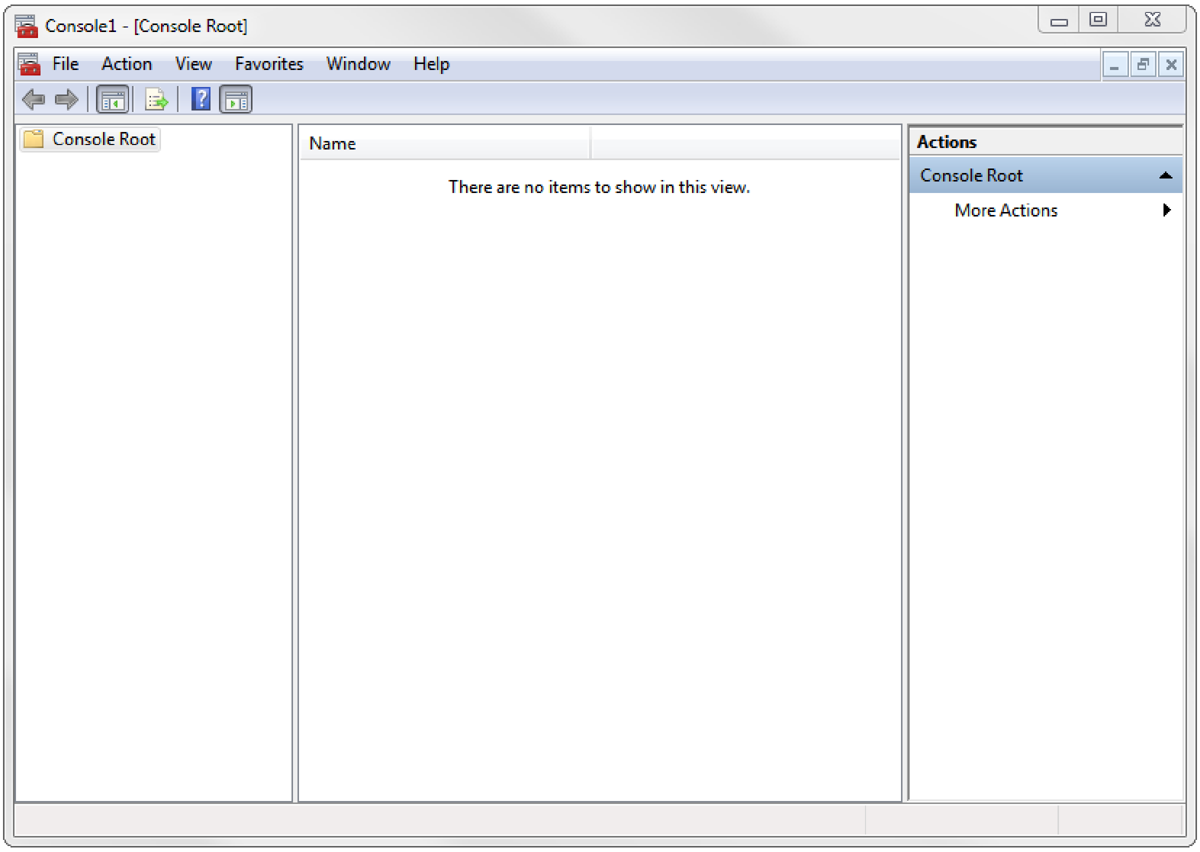
Use a CA certificate customized in case of error on proxy: here is possible *import/export the CA* used when there be an error in the remote certificate validation. When the *use CA of error* is not checked, the option of view the CA of error will be disabled.

Importing the X.509 certificate on Windows

Importing the certificate in the Windows base will have effect in all applications that query this base, in this list we have the following applications:

- Internet Explorer;
- Google Chrome;
- Windows live messenger (MSN).

1. Open the Microsoft Management Console. Access the Start menu**,** select **Run,** type **mmc,** and click on **OK**.

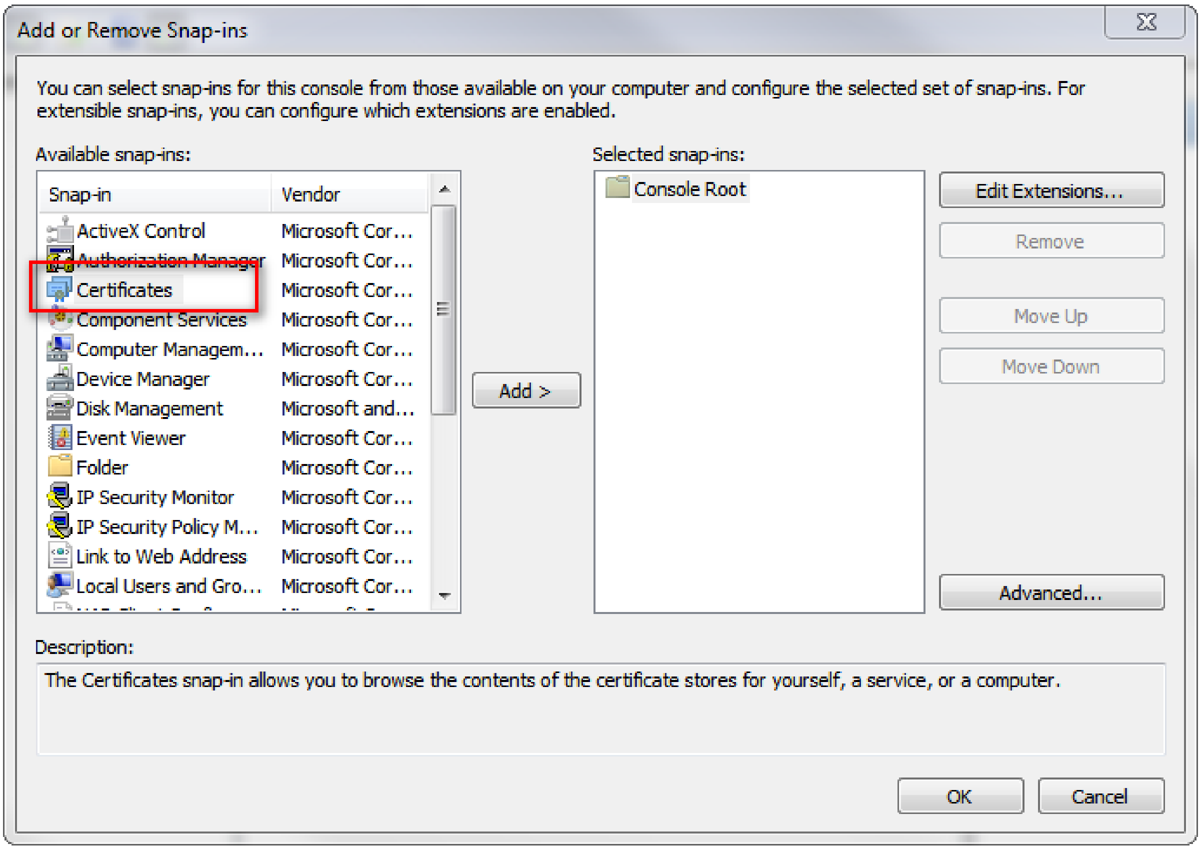

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Name
Actions
Console Root
More Actions

There are no items to show in this view.

Image 468 – Microsoft Management Console.

2. On the MMC screen click on **File,** then click on **Add/Remove snap-in.**

3. Select the option **Certificates,** then click on **Add.**



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Available snap-ins:
Selected snap-ins:
Console Root
Add >
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
OK
Cancel

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Image 469 – Add or remove Snap-is.

4. Select the option **Computer account**, and then select **Local Computer.**

5. On **Certificates > Trusted Root Certification Authorities > Certificates** right-click on **All tasks** and select **Import.**

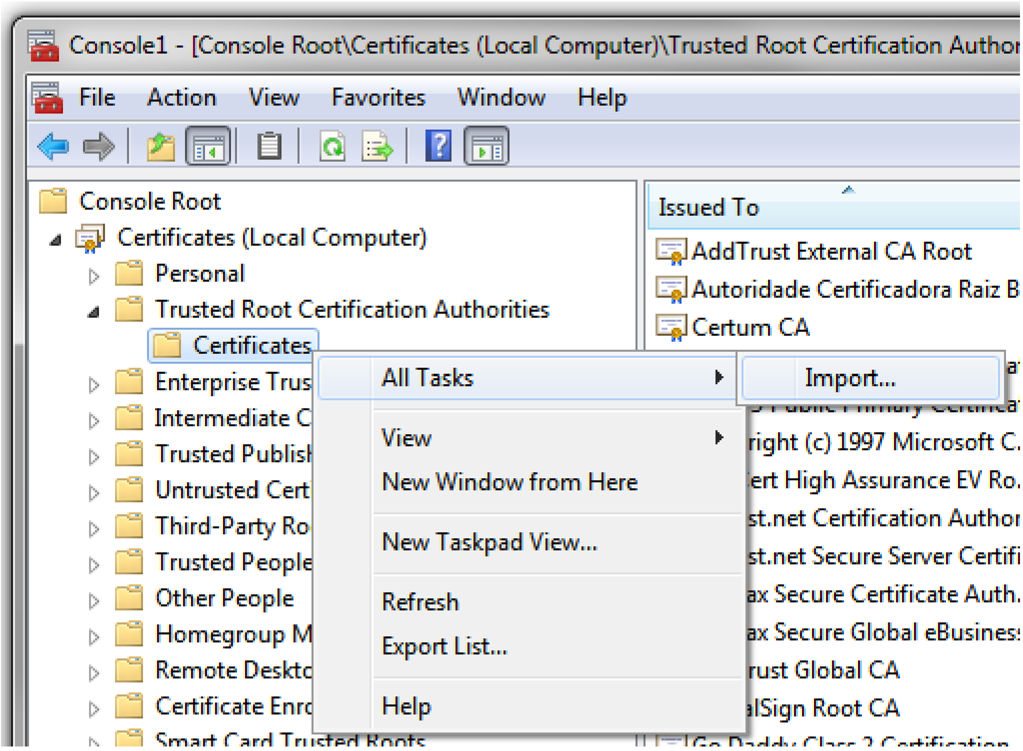
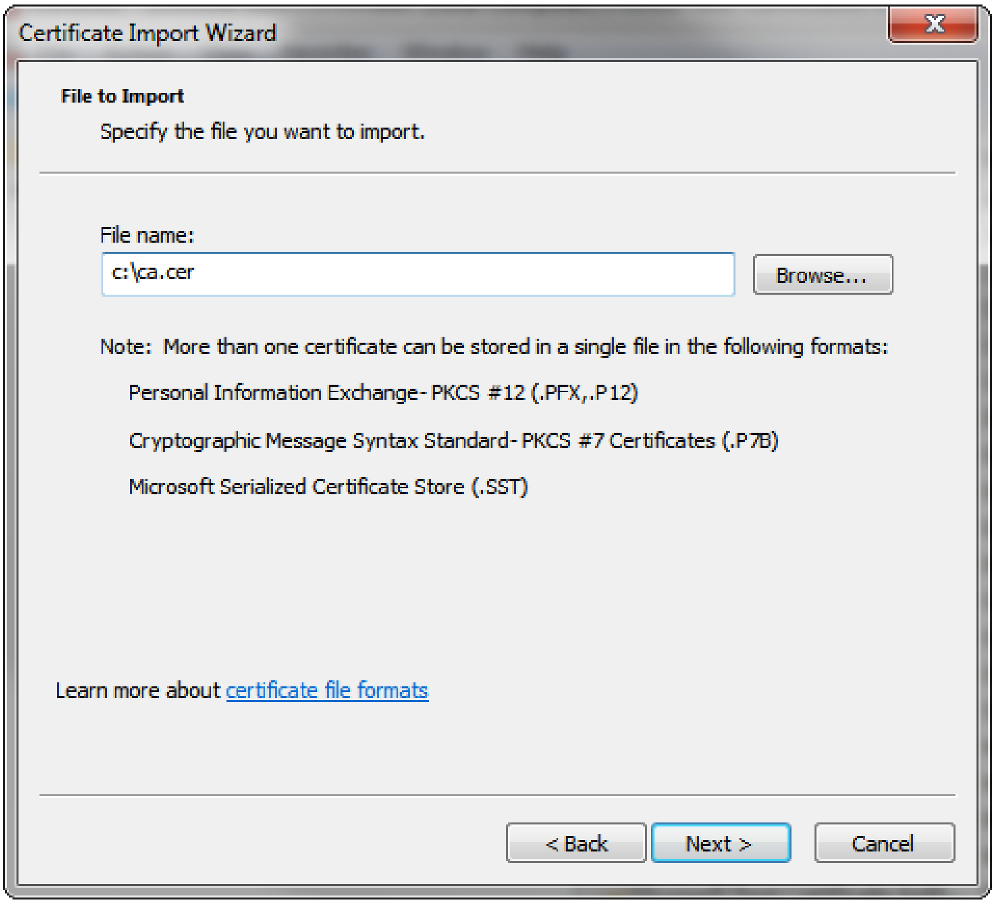

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Author
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trus
Intermediate C
Trusted Publish
Untrusted Cert
Third-Party Ro
Trusted People
Other People
Homegroup M
Remote Deskto
Certificate Enro
Smart Card Trusted Roots
Issued To
AddTrust External CA Root
Autoridade Certificadora Raiz B
Certum CA
right (c) 1997 Microsoft C.
ert High Assurance EV Ro.
st.net Certification Author
st.net Secure Server Certifi
ax Secure Certificate Auth.
ax Secure Global eBusines
rust Global CA
lSign Root CA
Go Daddy Class 2 Certification
All Tasks
Import...
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

Image 470 – Microsoft Management Console – certificates, all taks, and import).

6. Select the X.509 file, i.e. the file with **.cer. extension**


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
< Back
Next >
Cancel

File name: c:\ca.cer

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Image 471 – Specifying the directory where you are importing the file.

Importing X.509 certificate on Mozilla Firefox

1. Click on **Tools > Options**

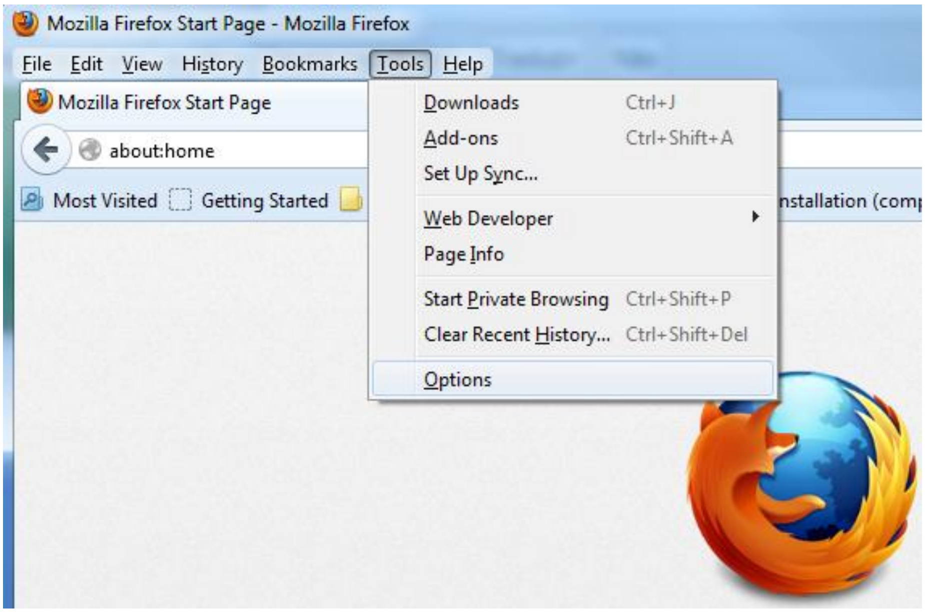
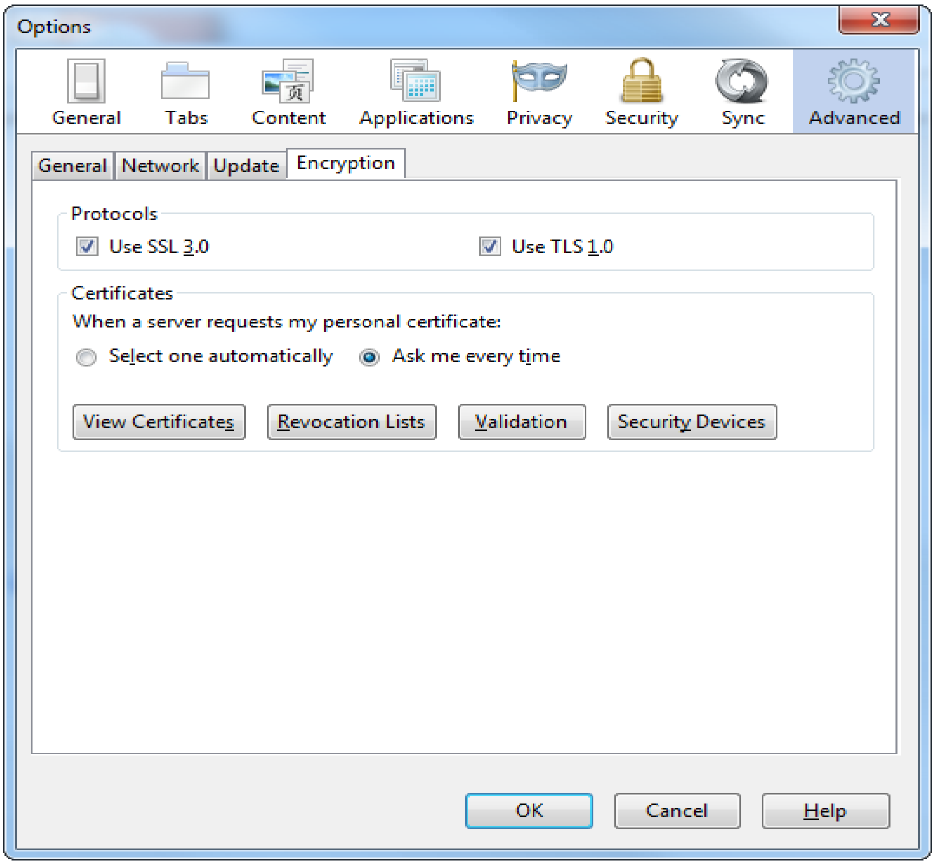

Mozilla Firefox Start Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Mozilla Firefox Start Page
about:home
Most Visited Getting Started
Downloads Ctrl+J
Add-ons Ctrl+Shift+A
Set Up Sync...
Web Developer
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options

Image 472 – Mozilla Firefox (import certificate).

2. Select the option **Advanced > encryption**

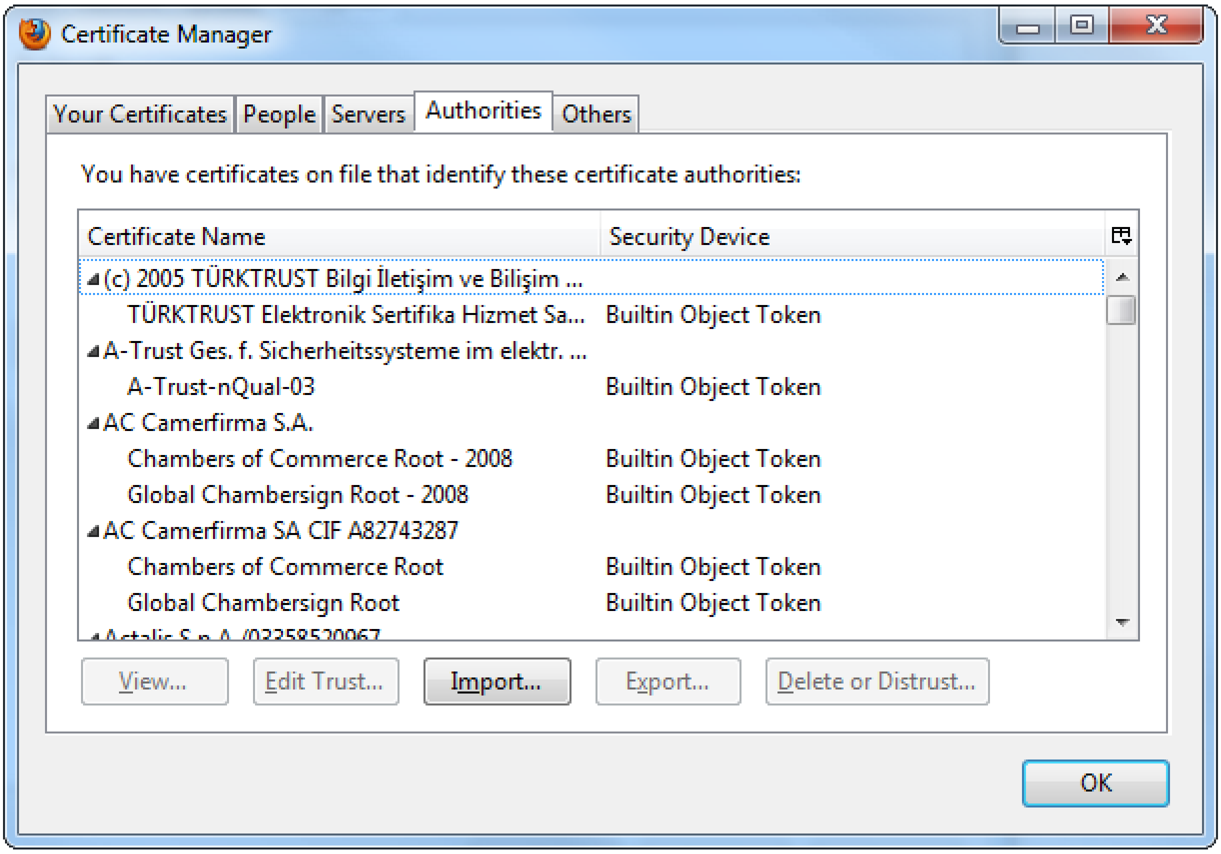

Options
General Tabs Content Applications Privacy Security Sync Advanced
General Network Update Encryption
Protocols
Certificates
View Certificates
Revocation Lists
Validation
Security Devices
OK
Cancel
Help

☑ Use SSL 3.0
☑ Use TLS 1.0

When a server requests my personal certificate:
○ Select one automatically ● Ask me every time

Image 473 – Mozilla Firefox (encryption).

3. Select the option **View Certificates,** in the *Certificate Manager* screen select the *Authorities tab* and click on **Import**.



Certificate Manager
Your Certificates
People
Servers
Authorities
Others

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim ...	
TÜRKTRUST Elektronik Sertifika Hizmet Sa...	Builtin Object Token
A-Trust Ges. f. Sicherheitssysteme im elektr. ...	
A-Trust-nQual-03	Builtin Object Token
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token
Global Chambersign Root	Builtin Object Token

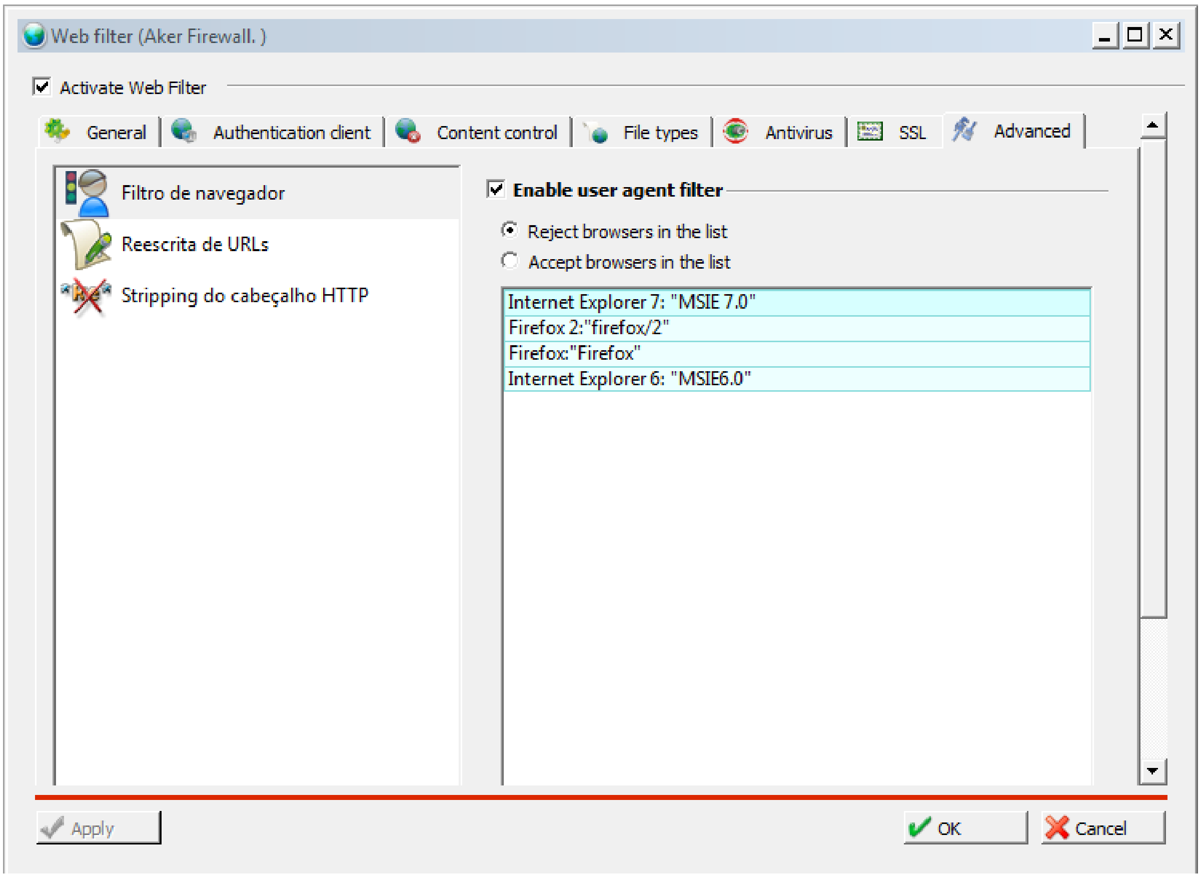
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK

Image 474 – Certificate Manager – Authorities.

4. Select the X.509 file, i.e., the file with **.cer. extension.**

Advanced tab

- **User agent Filter**


Web filter (Aker Firewall.)
General
Authentication client
Content control
File types
Antivirus
SSL
Advanced
Filtro de navegador
Reescrita de URLs
Stripping do cabeçalho HTTP
Apply
OK
Cancel

☑ Activate Web Filter

☑ **Enable user agent filter**

● Reject browsers in the list
○ Accept browsers in the list

Internet Explorer 7: "MSIE 7.0"
Firefox 2:"firefox/2"
Firefox:"Firefox"
Internet Explorer 6: "MSIE6.0"

Image 475 – Web Filter: Advanced.

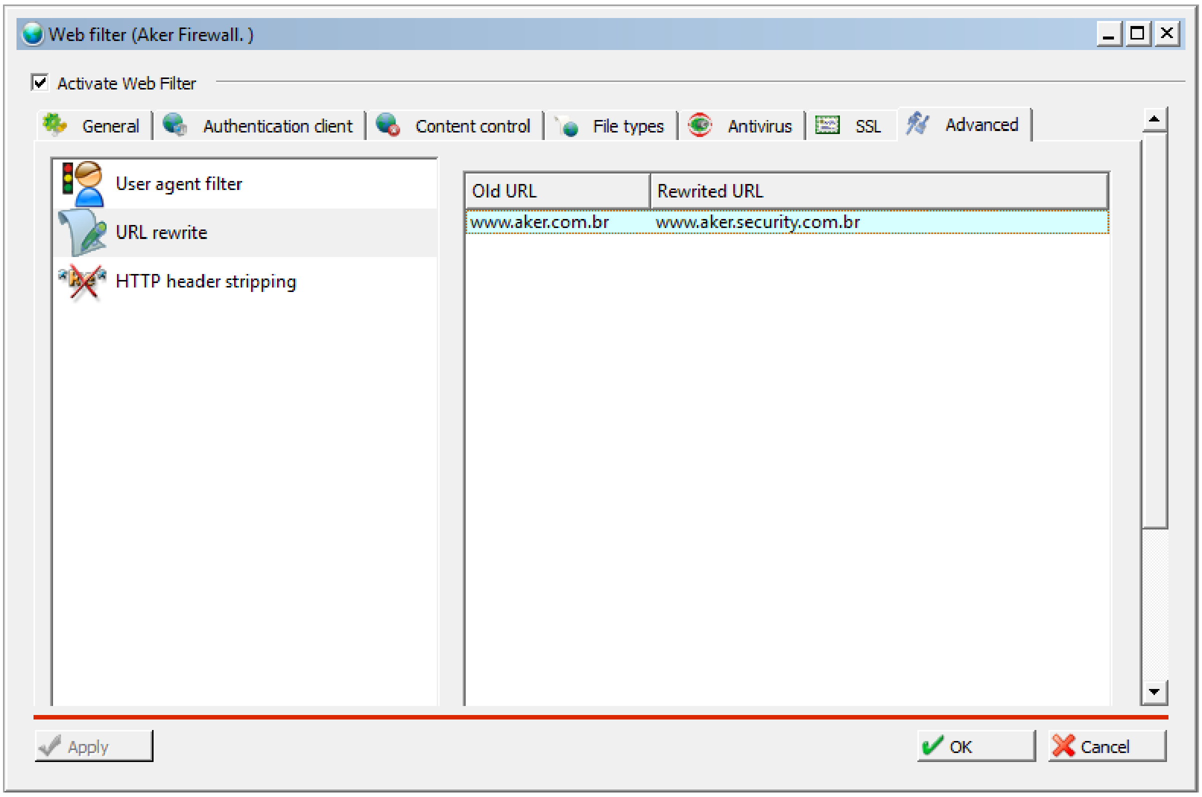
Selecting the **Enable user agent filter** option, allows the user to accept or reject the browsers inserted in the list.

This list is created by the user and in it shall be inserted several types of browsers you wish to block or grant access, below follows an example of how these browsers shall be inserted:

- Internet Explorer 6: " **MSIE 6.0** ";
- Internet Explorer 7: " **MSIE 7.0";**
- Internet Explorer (any): " **MSIE** ";
- Media Player: " **Windows-Media-Player** ";
- Firefox: " **Firefox** ";
- Firefox 2: " **Firefox/2** ".

The browser validation is done *before* the header stripping, this way it is possible to replace the version for a fixed string without losing this filtering.

- **URL rewrite**



Web filter (Aker Firewall.)
General
Authentication client
Content control
File types
Antivirus
SSL
Advanced
User agent filter
URL rewrite
HTTP header stripping
Apply
OK
Cancel

☑ Activate Web Filter

Old URL	Rewrited URL
www.aker.com.br	www.aker.security.com.br

Image 476 – Web Filter: Advanced.

URL rewrite is similar to website redirection. It is a web server internal process that works in a transparent way resolving the broken links problem on websites.

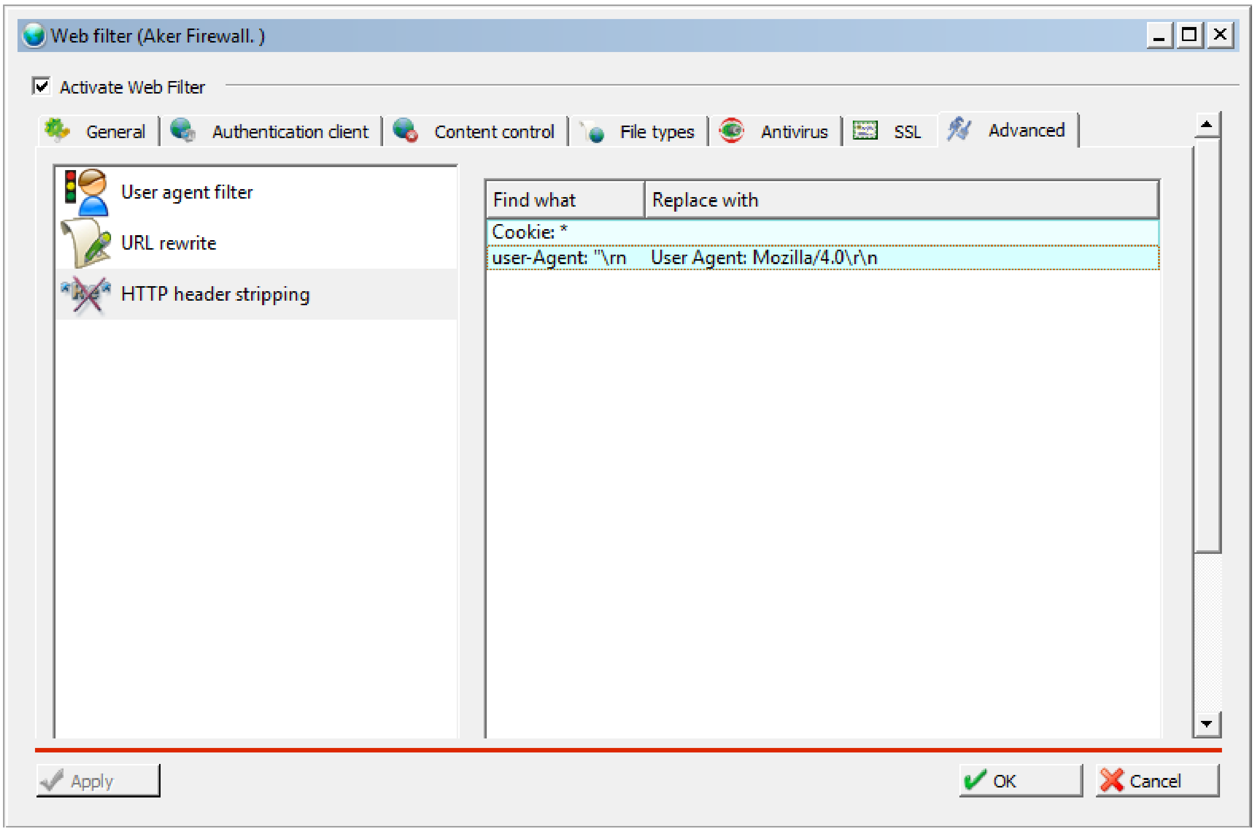
On the Old URL column as the name says, the address that will be translated to a new one (Rewritten URL) shall be informed.

Below follows the example:

Old URL: www.aker.com.br

Rewritten URL: www.aker.security.com.br

- **HTTP header stripping**


Web filter (Aker Firewall.)
☑ Activate Web Filter
General
Authentication client
Content control
File types
Antivirus
SSL
Advanced
User agent filter
URL rewrite
HTTP header stripping
Apply
OK
Cancel

Find what	Replace with
Cookie: *	
user-Agent: "\rn	User Agent: Mozilla/4.0\r\n

Image 477 – Web Filter: advanced.

This option allows removing and changing Header’s part, increasing the internal security.

Header stripping operation: all lines of HTTPS header are compared individually with all registered expressions. Header stripping works only in the client header removal for the server.

Header Stripping is performed right after the client’s browser version is verified and *before* the other proxy HTTP process, so proxy will treat the header modified version as it has been sent by the client.

Follows below the example of how to fill in the fields*: Find what* and *Replace with.*

To remove Cookies (no quotes):

Find what: " **Cookie: *** " – Replace with: "" (nada).

To hide clients’ browser version:
Find what: " **User-Agent: *\r\n** " – Replace with: " **User Agent: Mozilla/4.0\r\n**".

Header stripping configuration must be done very carefully because it can stop the use of Internet.

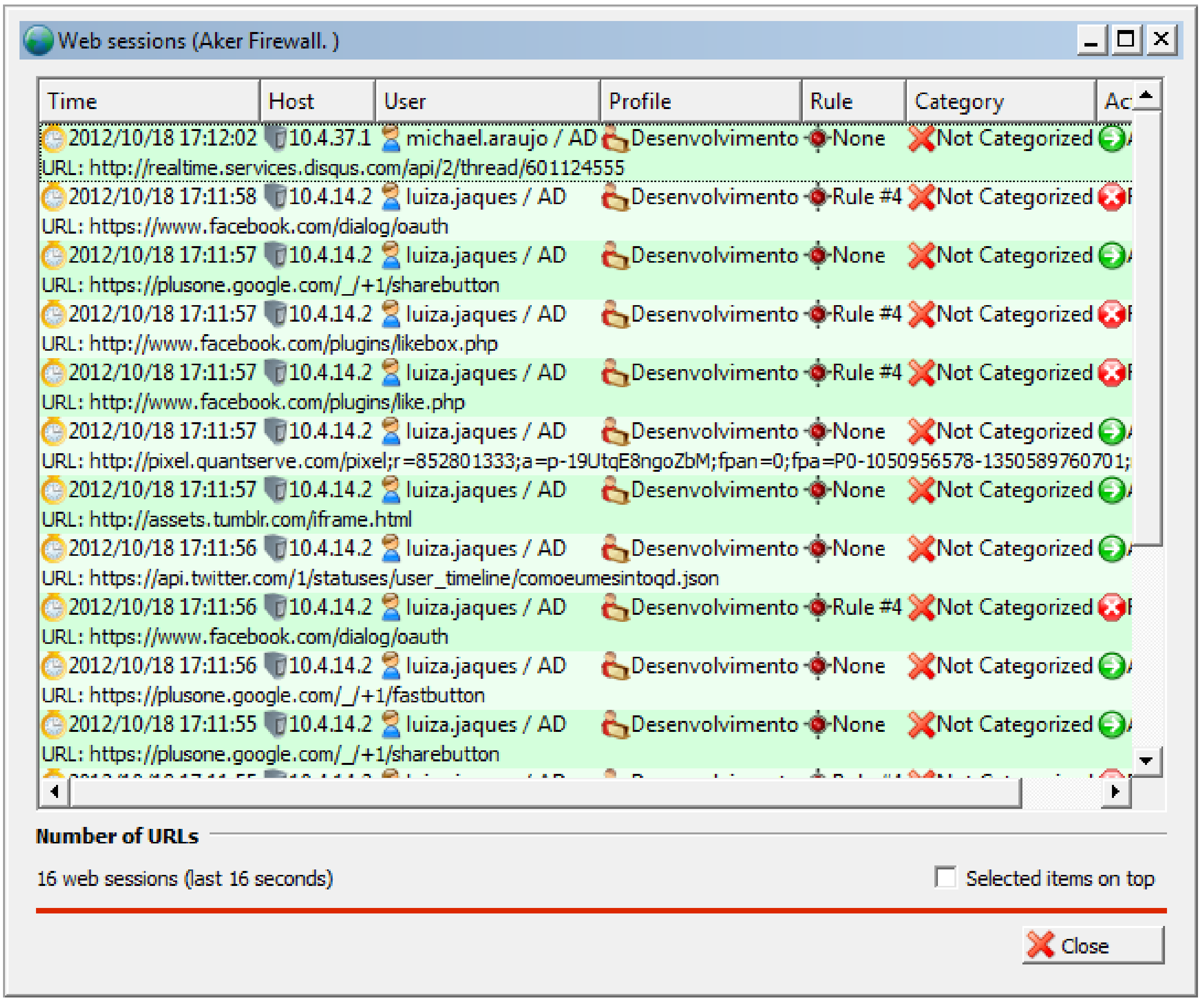
When you are replacing a line you must to always remember to add **\r\n** at the end (" **User-Agent: *\r\n** ")

30.3. Editing Web session parameters

Web sessions

This window allows the administrator view the active sessions verifying what has been accessed and who has accessed it, the time is defined in the *Web Filter* menu, *General* tab, *Web sessions timeout* option.

To gain access to the Web sessions window follow the steps below:



Time	Host	User	Profile	Rule	Category	Ac
2012/10/18 17:12:02	10.4.37.1	michael.araujo / AD	Desenvolvimento	None	Not Categorized	
URL: http://realtime.services.disqus.com/api/2/thread/601124555						
2012/10/18 17:11:58	10.4.14.2	luiza.jaques / AD	Desenvolvimento	Rule #4	Not Categorized	
URL: https://www.facebook.com/dialog/oauth						
2012/10/18 17:11:57	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: https://plusone.google.com/_/+1/sharebutton						
2012/10/18 17:11:57	10.4.14.2	luiza.jaques / AD	Desenvolvimento	Rule #4	Not Categorized	
URL: http://www.facebook.com/plugins/likebox.php						
2012/10/18 17:11:57	10.4.14.2	luiza.jaques / AD	Desenvolvimento	Rule #4	Not Categorized	
URL: http://www.facebook.com/plugins/like.php						
2012/10/18 17:11:57	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: http://pixel.quantserve.com/pixel;r=852801333;a=p-19UtqE8ngoZbM;fpan=0;fpa=P0-1050956578-1350589760701;						
2012/10/18 17:11:57	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: http://assets.tumblr.com/iframe.html						
2012/10/18 17:11:56	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: https://api.twitter.com/1/statuses/user_timeline/comoeumesintoqd.json						
2012/10/18 17:11:56	10.4.14.2	luiza.jaques / AD	Desenvolvimento	Rule #4	Not Categorized	
URL: https://www.facebook.com/dialog/oauth						
2012/10/18 17:11:56	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: https://plusone.google.com/_/+1/fastbutton						
2012/10/18 17:11:55	10.4.14.2	luiza.jaques / AD	Desenvolvimento	None	Not Categorized	
URL: https://plusone.google.com/_/+1/sharebutton						

Number of URLs

16 web sessions (last 16 seconds)

☐ Selected items on top

Image 478 – Sessões Web.

- Click on the *Information* menu;

- Select *Web sessions*

The description of the Web sessions information fields:

Time: Indicates day, time, and URL that has been accessed.

Host: Indicates the host where the URL has been accessed.

User: Indicates the user who has accessed the URL.

Profile: Indicates which access profile the user has been directed to when attempting to access an URL.

Rule: Indicates which access rule the URL has fit.

Category: Indicates which category the URL has fit.

Action: Indicates if the web sessions that have passed through the firewall have been accepted or rejected.

Configuring Socks proxy

31. Configuring Socks proxy

This chapter shows what is and how to configure the Socks proxy.

31.1. Planning the installation

What is Aker Firewall Socks proxy?

The SOCKS proxy is a specialized program of Aker Firewall, designed to work with programs that support the SOCKS protocol, version 4 or 5.

The main function of SOCKS proxy is to provide a better security level for protocols to pass through the firewall, especially complex protocols which use more than one connection. It is possible, through the use of the SOCKS 5, to perform user authentication for any services that pass through the firewall, even without the authentication client.

It is a non-transparent proxy (for more information, see the chapter titled **Working with proxies**), therefore, the clients that will use it must have proxy support and must be configured to use a proxy.

Using SOCKS proxy

To use the SOCKS proxy of Aker Firewall, it is necessary to follow these steps:

1. Create the desired access profiles and associate them with the desired users and groups. This is explained in the chapter **User access profiles**)
2. Edit the configuration parameters of SOCKS proxy (this will be displayed in the section **Editing the parameters of the SOCKS proxy**).
3. Create a filtering rule allowing the client hosts to access the proxy (for more information, see the chapter titled **stateful filter**).

The SOCKS proxy of Aker Firewall listens to connections on port 1080, using the TCP protocol. If necessary, this number can be changed to any port, by adding the parameter **-p** ***port***, where *port* is the number of the desired port, on the proxy startup. The proxy is started from the file **/etc/firewall/rc.aker**, and its initialization string may be changed from **/etc/firewall/fwsocksd** to **/etc/firewall/fwsocksd -p 8080**, for example.

31.2. Editing the parameters of SOCKS proxy

To use the SOCKS proxy, it is necessary to define some parameters that will determine the basic characteristics of its operation. This definition is made in the SOCKS proxy configuration window.

To gain access to the Socks proxy window follow the steps below:

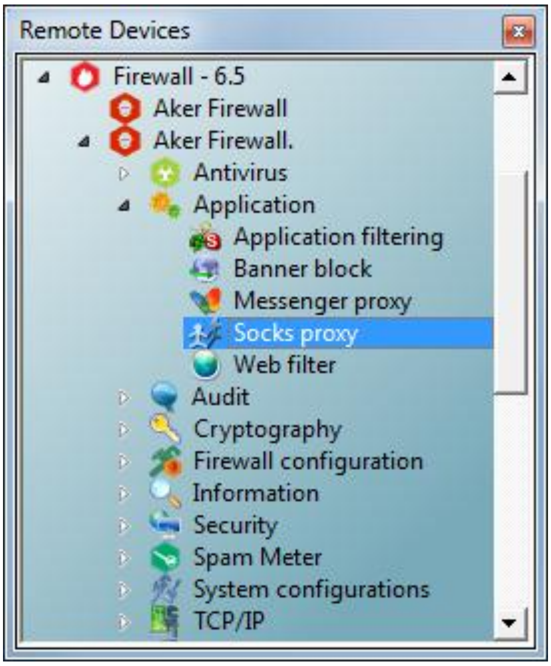
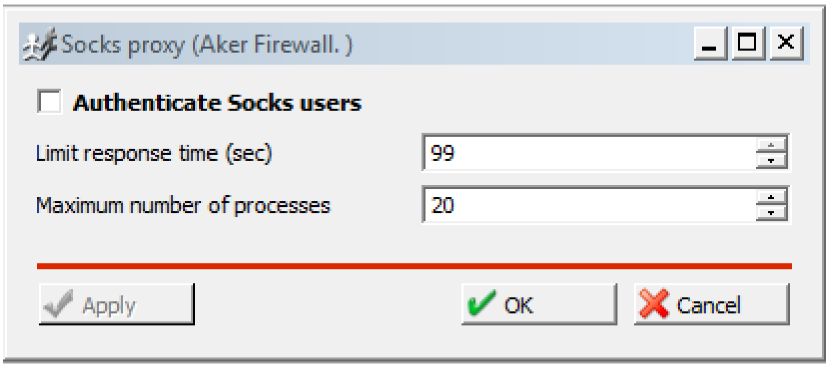

Remote Devices
Firewall - 6.5
Aker Firewall
Aker Firewall.
Antivirus
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP

Image 479 – access window: Socks proxy

- Click on the *Application* menu.
- Select *Socks proxy.*

SOCKS Proxy configuration parameters


Socks proxy (Aker Firewall.)
Apply
OK
Cancel

☐ **Authenticate Socks users**

Limit response time (sec): 99

Maximum number of processes: 20

Image 480 – Socks users authentication

- The **OK** button will close the SOCKS proxy configuration window and save all changes.

- The **Apply** button saves all modifications but keeps the window open
- The **Cancel** button will close the configuration window and discard all the changes done

The meaning of the parameters:

Authenticate SOCKS users: This field enables or not the user authentication of the SOCKS proxy. If it is checked, every time that a user tries to initiate a session, he will be asked for an identification and a password, and the session will only be started if the user is authenticated by any of the authenticators.

If the user is using Aker Authentication Client and has an established session with the firewall, then no username and password will be asked, that is, the proxy will behave like no users authentication is being performed; however it is doing it. If the Aker Authentication Client session is closed, then the proxy will ask for a username and a password in the next access (For more information about Aker Authentication Client, see the chapter titled Aker authentication client).

The version 4 of the SOCKS protocol does not support user authentication, thus the only way to authenticate users using this protocol version is with the use of the authentication client. If this option is checked, the version supported by the client is 4 and there is no access profile session active, then the firewall will refuse all clients' requests.

Limit response time: This parameter defines the maximum amount of time, in seconds, that the proxy waits for client data, from the moment that a new connection is established. If this time is reached without the necessary data from the client, the connection will be closed.

Maximum number of processes: This field defines the maximum number of processes of the SOCKS proxy can be active simultaneously. Since each process treats a single connection, this field also defines the maximum number of requests that can be treated simultaneously.

Configuring the RPC and DCE-RPC Proxy

32. Configuring the RPC proxy and DCE-RPC proxy

This chapter shows how to configure the RPC and DCE-RPC proxy.

What is the RPC proxy?

RPC proxy is a specialized program of Aker Firewall to work with the RPC protocol, being more specific the SUN RPC.

In computer science, a **remote procedure call** (**RPC**) is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction. That is, the programmer writes essentially the same code whether the subroutine is local to the executing program, or remote. When the software in question uses object-oriented principles, RPC is called **remote invocation** or **remote method invocation**.

It is a transparent proxy (for more information see the chapter titled **Working with proxies**), this way both client and server do not know about its existence.

Using the RPC *proxy*

To use the RPC proxy, it is necessary to follow the steps bellow:

- Create a service that will be disabled for the RPC proxy, and edit the context parameters that are going to be used by this service (for more information see the chapter titled **Registering Entities**);
- Add a filtering rule allowing the service created above be used to networks or hosts at your choice (for more information see the chapter titled **Stateful inspection**).

What is the DCE-RPC proxy?

DCE- RPC proxy is a specialized program of Aker Firewall to work with the RPC protocol, being more specific the DCE- RPC.

DCE/RPC, short for "Distributed Computing Environment / Remote Procedure Calls", is the remote procedure call system developed for the Distributed Computing Environment (DCE). This system allows programmers to write distributed software as if it were all working on the same computer, without having to worry about the underlying network code.

It is a transparent proxy (for more information see the chapter titled **Working with proxies**), this way both client and server do not know about its existence**.**

Using the DCE-RPC proxy

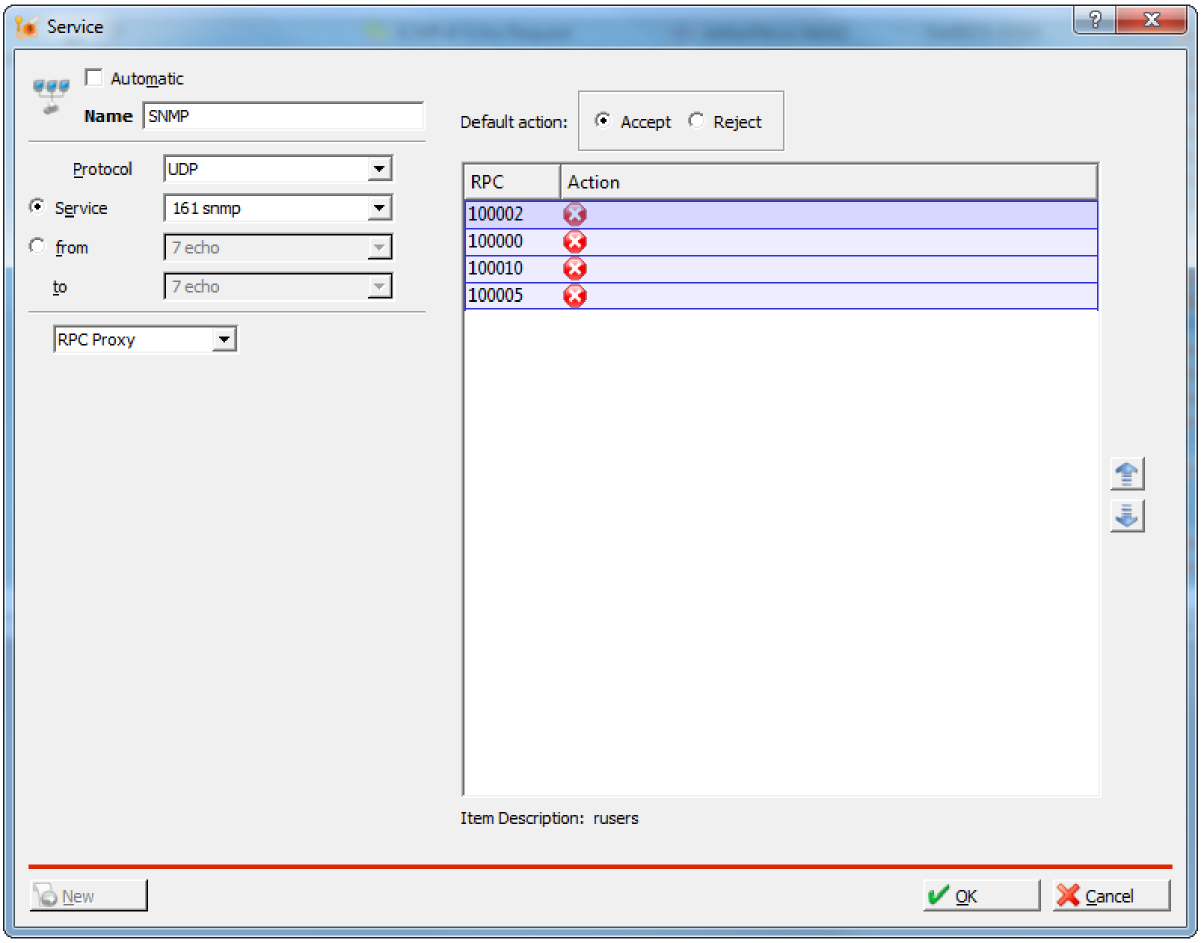
To use the RPC proxy, it is necessary to follow the steps bellow:

- Create a service that will be disabled for the DCE-RPC proxy, and edit the context parameters that are going to be used by this service (for more information see the chapter titled **Registering Entities**);
- Add a filtering rule allowing the service created above be used to networks or hosts at your choice (for more information see the chapter titled **Stateful inspection**).

32.1. Editing the parameters of a RPC context

The configuration window of a DCE-RPC will be displayed when you select the UDP protocol and the RPC Proxy option in the service edition window.

Configuration window of a RPC context



Name SNMP

Protocol UDP

● Service 161 snmp

○ from 7 echo

to 7 echo

RPC Proxy

Default action: ● Accept ○ Reject

RPC	Action
100002	✗
100000	✗
100010	✗
100005	✗

Item Description: rusers

Image 481 – Configuration of a RPC context.

In the window above the parameters of a context associated to a specific service is configured. It consists of the following fields:

Default action: Indicate the action that will be applied to all remote services that are not present in the whitelist. It has two options *accept* and *reject*.

Whitelist: Sets individually the permissions of access to remote services.

Right-click on the RPC column will present you the following menu:

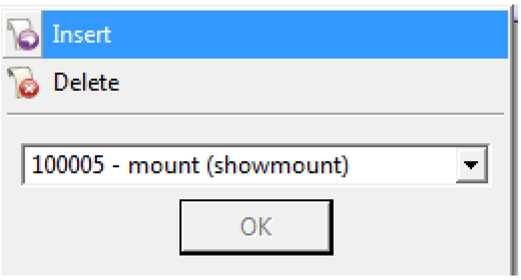

Insert
Delete
100005 - mount (showmount)
OK

Image 482 – RPC option menu.

- **Insert:** Adds a new service in the list.
- **Delete:** Removes the selected service from the list.
- **List of services:** Contains a predefined list of services and its numbers. It is possible to add services that are not on the list, simply clicking on the field right below delete where a code and the service will be displayed, and type the code of your choice.

The following menu change the Action; Reject or Accept

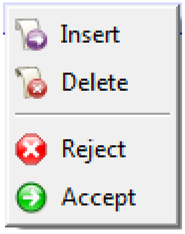
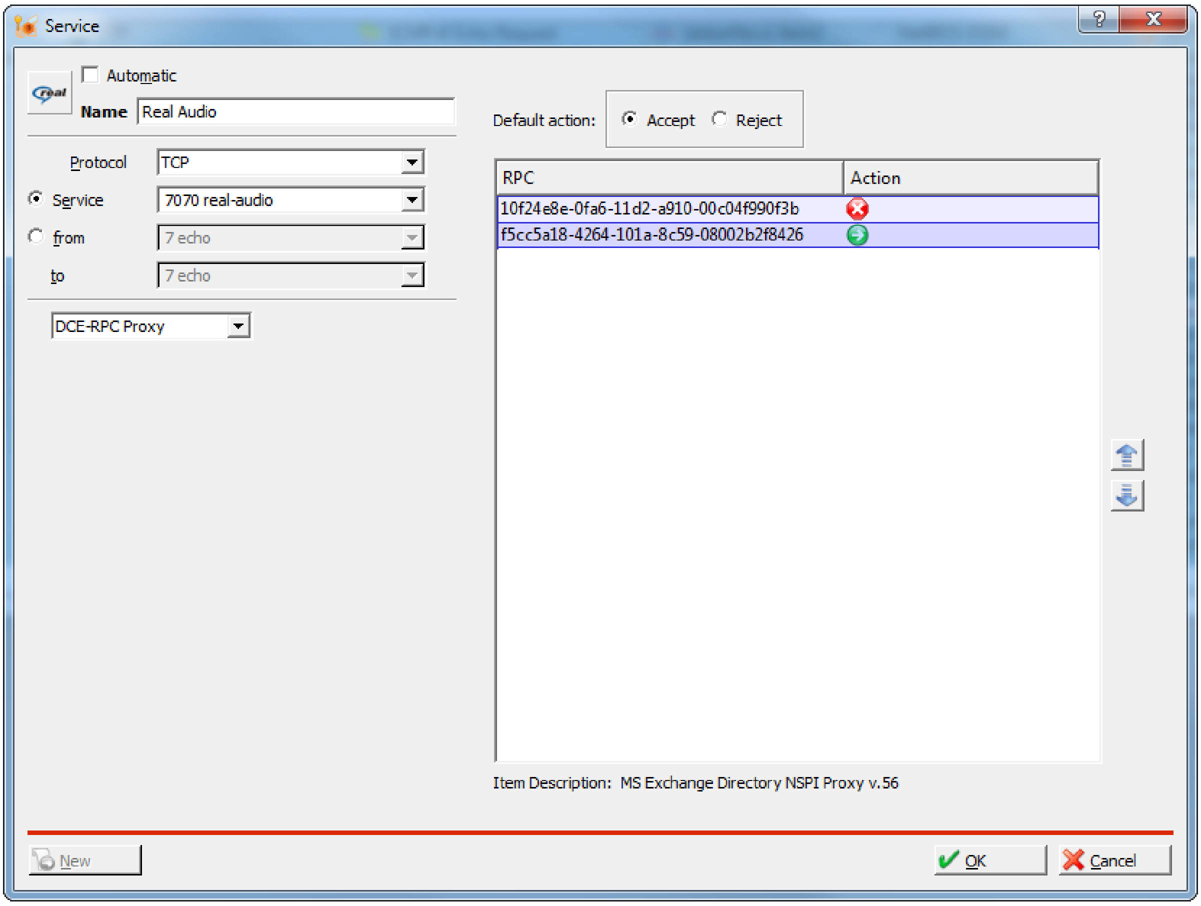

Insert
Delete
Reject
Accept

Image 483 – RPC option menu.

Editing the parameters of a DCE-RPC context

The configuration window of a DCE-RPC will be displayed when you select the UDP protocol and the RPC Proxy option in the service edition window.

Configuration window of a DCE-RPC context



☐ Automatic

Name Real Audio

Protocol: TCP

● Service: 7070 real-audio

○ from: 7 echo

to: 7 echo

DCE-RPC Proxy

Default action: ● Accept ○ Reject

RPC	Action
10f24e8e-0fa6-11d2-a910-00c04f990f3b	✗
f5cc5a18-4264-101a-8c59-08002b2f8426	✓

Item Description: MS Exchange Directory NSPI Proxy v.56

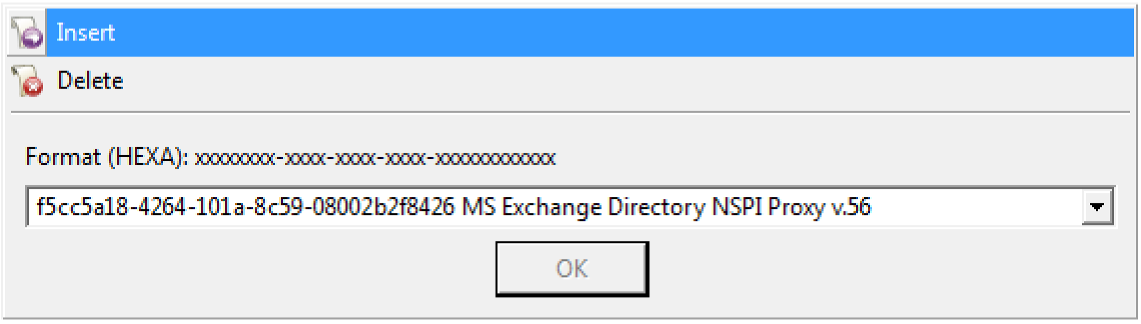
Image 484 – Configuration of a DCE-RPC context.

In the window above the parameters of a context associated to a specific service is configured. It consists of the following fields:

Default action: Indicate the action that will be applied to all remote services that are not present in the whitelist. It has two options *accept* and *reject*.

Whitelist: Sets individually the permissions of access to remote services.

Right-click on the RPC column will present you the following menu:



Format (HEXA): xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

f5cc5a18-4264-101a-8c59-08002b2f8426 MS Exchange Directory NSPI Proxy v.56

Image 485 – DCE-RPC option menu

- **Insert:** Adds a new service in the list.
- **Delete:** Removes the selected service from the list.
- **List of services:** Contains a predefined list of services and its numbers. It is possible to add services that are not on the list, simply clicking on the field right below delete where a code and the service will be displayed, and type the code of your choice.

The following menu change the Action; Reject or Accept

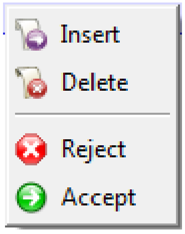


Image 486 – RPC option menu.

Configuring the MSN Proxy

33. Configuring the MSN proxy

This chapter shows what is for and how to configure the MSN proxy.

33.1. Planning the installation

What is the MSN Messenger?

Windows Live Messenger (formerly named **MSN Messenger**) is an instant messaging client created by Microsoft that is currently designed to work with Windows XP (up to Wave 3), Windows Vista, Windows 7, Windows Mobile, Windows Phone, Windows CE, Xbox 360, Blackberry OS, iOS, Java ME, S60 on Symbian OS 9.x, and Zune HD.[1] The client has been part of Microsoft's Windows Live set of online services since 2005. It connects to Microsoft Messenger service.

What is Aker Firewall MSN Messenger proxy?

This proxy main function is control MSM Messenger, allowing using this tool for the company benefit, avoiding the loss of productivity with employees using MSM Messenger to chat with friends, family, and etc., during work day, i.e. using this tool for purposes that are not of the company interest. Integrated to the access profile system, it will adapt to the company need, giving each user a specific privilege to you MSM Messenger.

Below follows few features of this program:

- It is integrated to the access profile system (allowing the control of users and groups).
- Defines whitelist and blacklists per profile.
- Controls the usage time.
- Controls the daily usage time (this option is configured on profiles) for each user.
- Controls the file sending/receiving (including by type).
- Controls invitations for other services such as video, audio, games, etc.).
- Performs a session log.

Using the MSN proxy

MSM Messenger default port is TCP 1863; however it also can be connected to servers through HTTP and SOCKS. Aker's MSN Proxy controls the data that will traffic through the transparent proxy (for more information see the chapter titled **Working with proxies**).

To use Aker Firewall MSN proxy follows the steps below:

1. Set MSN proxy generic parameters.
2. Create access profiles and associated them to users and groups at you choice (this has been described in the chapter titled **User access profile**).
3. Associate a filtering rule allowing users to use the MSN service (for more information see the chapter titled **Stateful inspection**).

33.2. Editing the MSN proxy parameters

To set the MSN proxy parameters follow the steps below:

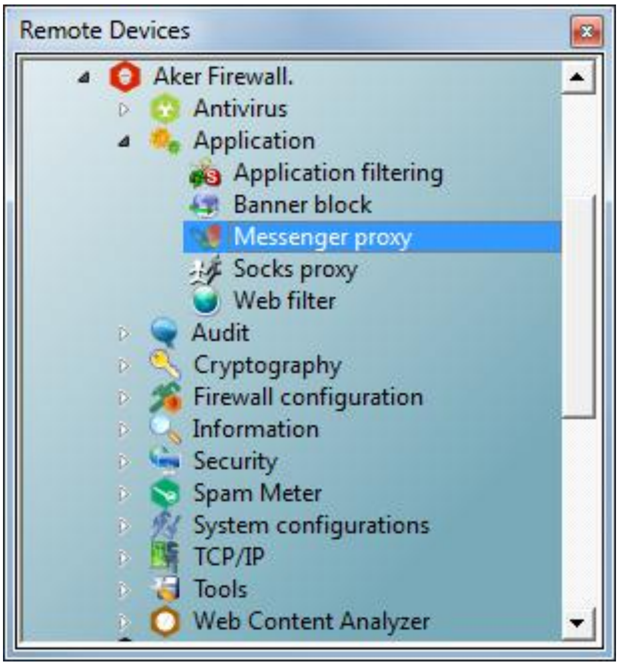

Remote Devices
Aker Firewall.
Antivirus
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer

Image 487 – Access window: Messenger proxy.

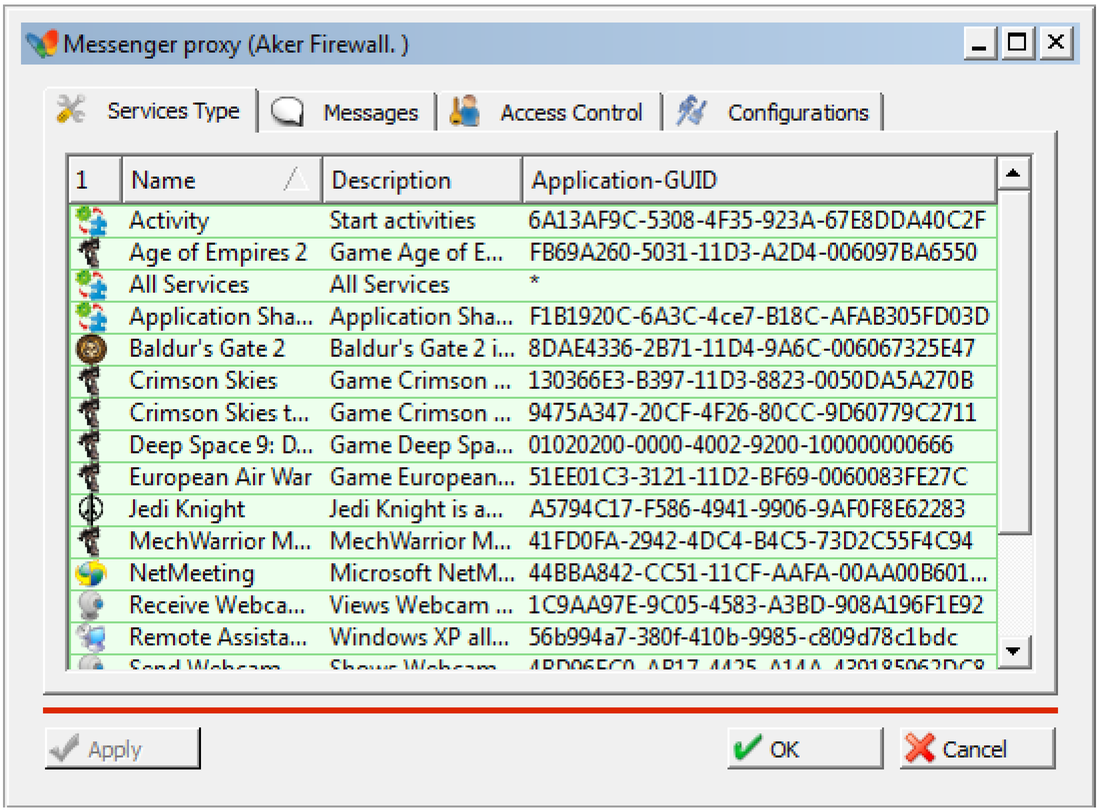
- Click on the *Application* menu
- Select *Messenger proxy*

MSN proxy configuration parameters window

- The **OK** button will close the MSN proxy window saving all changes.
- The **Apply** button will save all changes and keep the window opened.
- The **Cancel** button will discard all changes closing the window.

The Proxy Messenger window has four tabs, the description of each one them follows below:

Service type tab



1	Name	Description	Application-GUID
	Activity	Start activities	6A13AF9C-5308-4F35-923A-67E8DDA40C2F
	Age of Empires 2	Game Age of E...	FB69A260-5031-11D3-A2D4-006097BA6550
	All Services	All Services	*
	Application Sha...	Application Sha...	F1B1920C-6A3C-4ce7-B18C-AFAB305FD03D
	Baldur's Gate 2	Baldur's Gate 2 i...	8DAE4336-2B71-11D4-9A6C-006067325E47
	Crimson Skies	Game Crimson ...	130366E3-B397-11D3-8823-0050DA5A270B
	Crimson Skies t...	Game Crimson ...	9475A347-20CF-4F26-80CC-9D60779C2711
	Deep Space 9: D...	Game Deep Spa...	01020200-0000-4002-9200-100000000666
	European Air War	Game European...	51EE01C3-3121-11D2-BF69-0060083FE27C
	Jedi Knight	Jedi Knight is a...	A5794C17-F586-4941-9906-9AF0F8E62283
	MechWarrior M...	MechWarrior M...	41FD0FA-2942-4DC4-B4C5-73D2C55F4C94
	NetMeeting	Microsoft NetM...	44BBA842-CC51-11CF-AAFA-00AA00B601...
	Receive Webca...	Views Webcam ...	1C9AA97E-9C05-4583-A3BD-908A196F1E92
	Remote Assista...	Windows XP all...	56b994a7-380f-410b-9985-c809d78c1bdc

Image 488 – Messenger proxy – Service type tab.

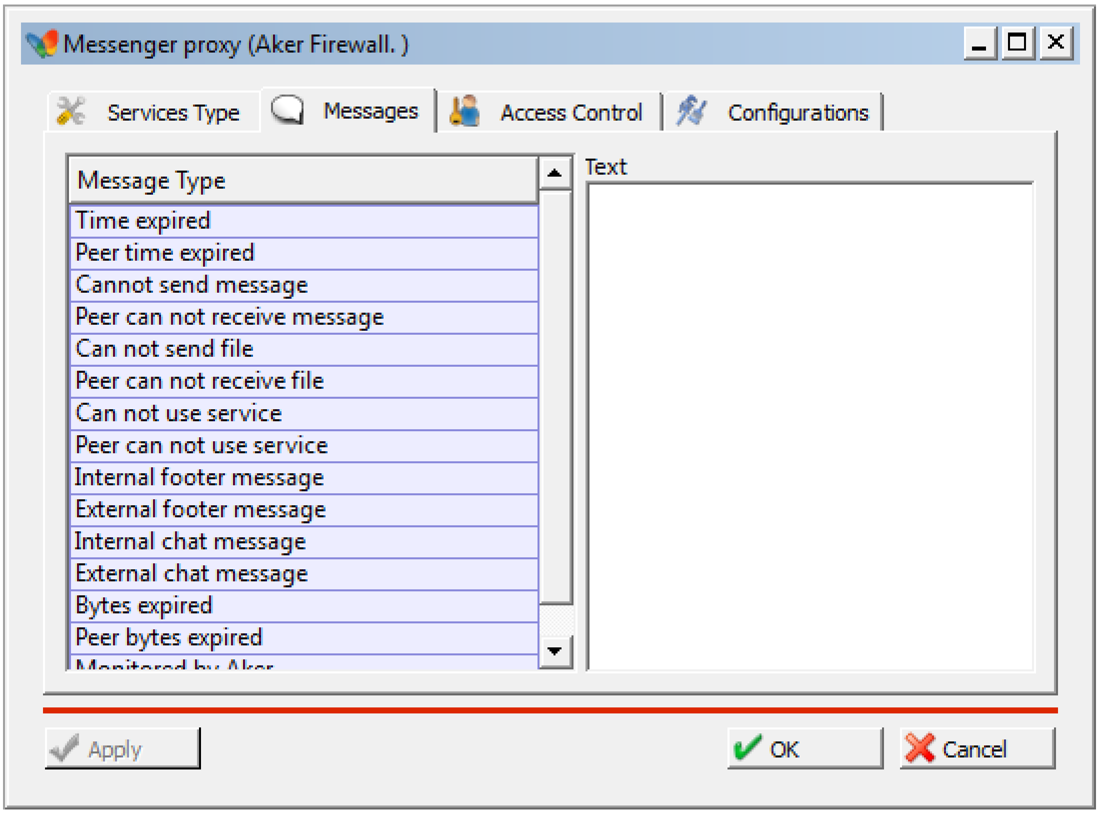
This tab sets extra services that will be available through the MSN connection. These services will be controlled by the profile rules of each user.

To add a new type of service, right-click and select the option **New**.

To remove a type of service, right-click and select the option **Delete.**

To edit any service, simply right-click on the service you wish to make any change, and you also can add several preconfigured services, clicking on the **Add default MSN service** option, which is located on the toolbar.

Messages tab

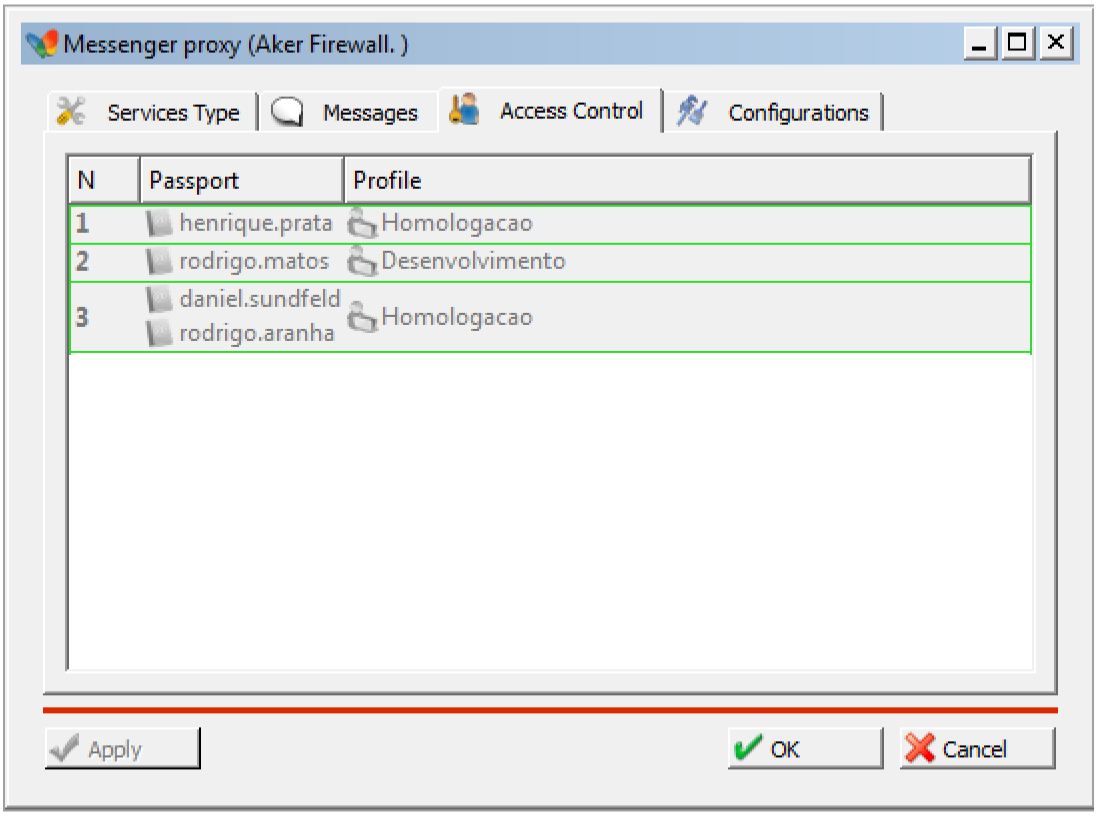

Messenger proxy (Aker Firewall.)
Services Type
Messages
Access Control
Configurations
Text
Apply
OK
Cancel

Message Type
Time expired
Peer time expired
Cannot send message
Peer can not receive message
Can not send file
Peer can not receive file
Can not use service
Peer can not use service
Internal footer message
External footer message
Internal chat message
External chat message
Bytes expired
Peer bytes expired

Image 489 – Messenger proxy – Messages tab.

This tab configures the messages that will be displayed to internal and external users when they do not have permission to perform a specific action through Messenger Proxy.

Access Control tab


Messenger proxy (Aker Firewall.)
Services Type
Messages
Access Control
Configurations
Apply
OK
Cancel

N	Passport	Profile
1	henrique.prata	Homologacao
2	rodrigo.matos	Desenvolvimento
3	daniel.sundfeld rodrigo.aranha	Homologacao

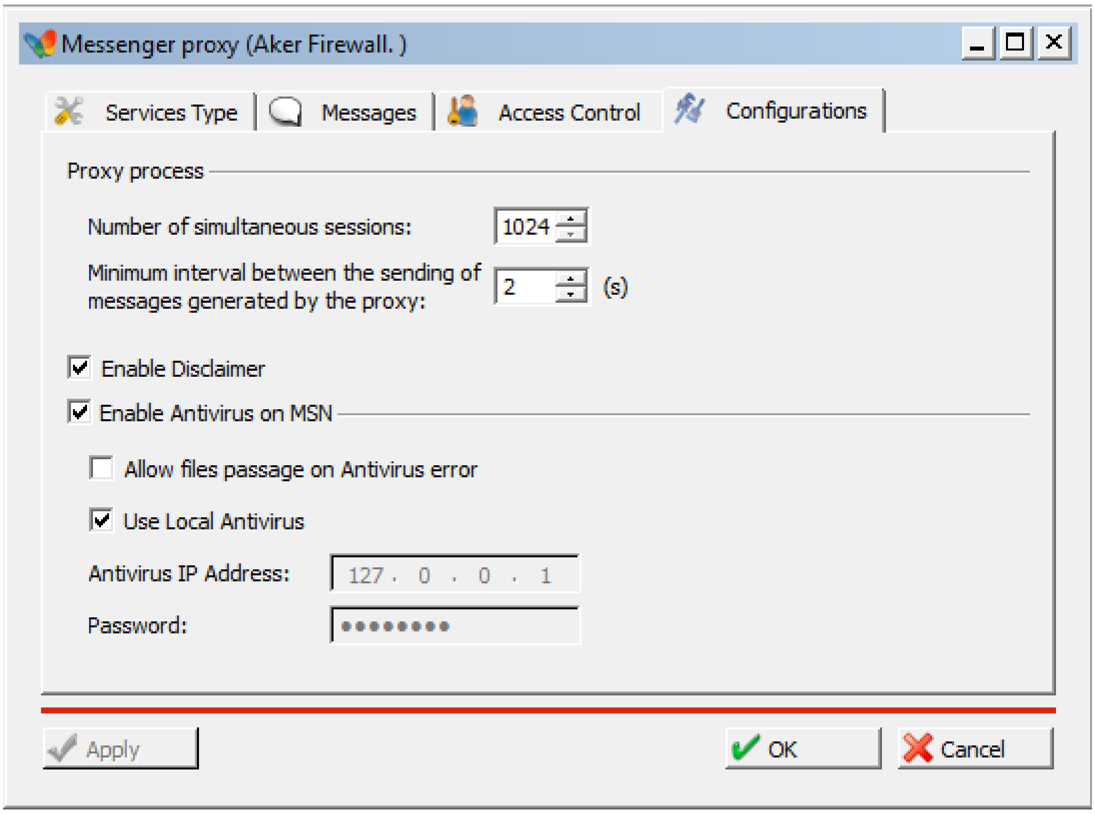
Image 490 – Messenger proxy – Access control.

This tab controls the users' access through the linking of a passport to a profile.

On *Passport*, an entity of type *e-mails list* will be selected (this option will be associated to a profile define in the Firewall).

E.g.*@aker.com.br --> profile "Test", this means that all users who have logged on MSN with addresses ending in *@aker.com.br* will be set automatically in this profile.

Configurations tab


Messenger proxy (Aker Firewall.)
Services Type
Messages
Access Control
Configurations
Apply
OK
Cancel

Proxy process

Number of simultaneous sessions: 1024

Minimum interval between the sending of messages generated by the proxy: 2 (s)

☑ Enable Disclaimer

☑ Enable Antivirus on MSN

☐ Allow files passage on Antivirus error

☑ Use Local Antivirus

Antivirus IP Address: 127 . 0 . 0 . 1

Password: ●●●●●●●●●

Image 491 – Messenger proxy – Configurations.

This tab configures the maximum about of sockets, and files that the MSN proxy can open. The default value is 1024, but it can go up to 8192.

Aker Firewall 6.5 has a virus scanning for transferred files. To activate this scanning check the option “**Enable Antivirus on MSN**”.

The option “**Allow files passage on Antivirus error”** allows transferring the infected files, in case the antivirus server is unavailable.

Check the option “**Use Local Antivirus**” to use the firewall antivirus, otherwise add the authentication and the IP address of your Antivirus server.

Configuring the Application filtering

34. Configuring the application filtering

This chapter shows how to configure the application filtering.

34.1. Planning the installation

What is the Application Filtering?

This filtering is based on the control of data which is passing through Aker Firewall. It is possible to analyze the protocol content and the type of files that are passing though, regardless the communication port that is being used.

Any packet that passes through the firewall or access profiles will be filtered, in special the following types:

- Download of specific file types via FTP, HTTP, and applications peer-to-peer.
- Connection of application control peer-to-peer (GNUTELLA, Napster, Kazaa, etc) and communication (Messenger, ICQ, etc.) upon any media (TCP or direct UDP and HTTP proxy).

Using the application filtering rule

To use Aker Firewall’s application filtering follow the steps bellow:

1. Create the desired filters.
2. Create filtering rules of global applications or desired access profiles.

34.2. Creating *Application filtering rules*

To gain access application filtering window follow the steps below:

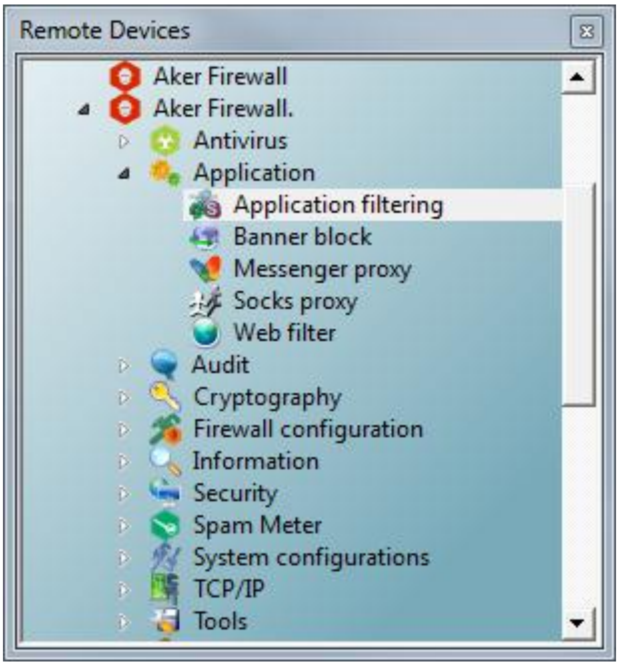
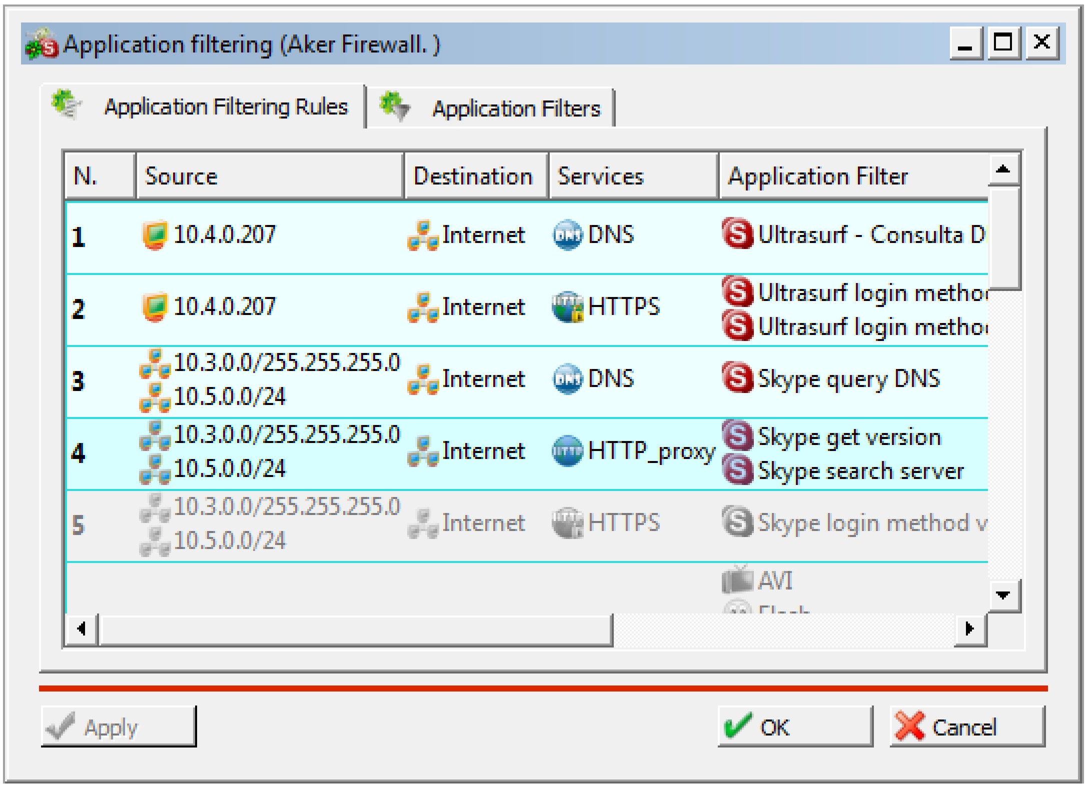

Remote Devices
Aker Firewall
Aker Firewall.
Antivirus
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 492 – access window: application filtering.

- Click on *Application* menu
- Select *Application filtering*

Application Filtering rules window


Application filtering (Aker Firewall.)
Application Filtering Rules
Application Filters
Apply
OK
Cancel

N.	Source	Destination	Services	Application Filter
1	10.4.0.207	Internet	DNS	Ultrasurf - Consulta D
2	10.4.0.207	Internet	HTTPS	Ultrasurf login metho Ultrasurf login metho
3	10.3.0.0/255.255.255.0 10.5.0.0/24	Internet	DNS	Skype query DNS
4	10.3.0.0/255.255.255.0 10.5.0.0/24	Internet	HTTP_proxy	Skype get version Skype search server
5	10.3.0.0/255.255.255.0 10.5.0.0/24	Internet	HTTPS	Skype login method v
				AVI

Image 493 – Application filtering – Application filtering rules.

This window has two tabs, one of them with the application filtering global rules definitions, and the other allowing the creation of filters that will be used in this rule and in the filtering rules of access profiles.

- The OK button will save all changes closing the window.
- The Apply button will save all changes and keep the window opened.
- The Cancel button will discard all changes closing the window.

Application filtering rules

This tab provides the application rules that will be used by the firewall. It is also possible to create specific rules to access profiles (for more information see the chapter titled **Registering access profiles**)

These rules allow the block of specific types of files according to its real type, regardless of its extension or protocol that is being used to send them. It is also possible; instead of blocking it, simply change the priority of a service or a type of file that is being transferred.

One of the important uses of this filter is the Internet access optimization. It is possible that users have fast access to the Internet, but whenever they attempt to download files which the types are not taken as important such as mp3, videos, etc., the connection that is being used to transfer these files will have its bandwidth automatically reduced.

Below follows the operation options menu for the *Application Filtering rules*:

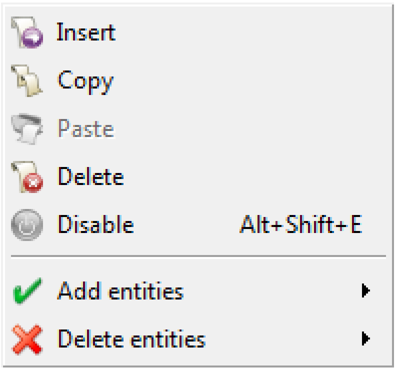


Image 494 – Option menu.

- **Insert:** Adds a new rule.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes a rule you have recently copied to the list.
- **Delete**: Deletes the selected rule.
- **Enable/Disable:** Enables/disables the selected rule.

Each rule consists of the following fields:

Source: Specifies the communications origins that the filter will be inspecting, to do it one or more entities of type: *machine, network, or set* need to be added (for more information see the chapter titled **Registering entities**).

Destination: Specifies the communication destination that the filter will be inspecting, to do it one or more entities of type: *machine, Network, or set* need to be added (for more information see the chapter titled **Registering entities**).

Services: Specifies the communication service that the filter will be inspecting, to do it one or more entities of type: *machine, Network, or set* need to be added (for more information see the chapter titled **Registering entities**).

Application Filter: Indicates the filters that are active for connections directed to one of the destination specified in the rule. The filters definition is done in the Application Filtering window. For more information see the chapter titled **Configuring the application filtering.**

Action: Indicates the action that will be taken by the firewall, in case one of the specified filters is applied. It has two options; the description of them follows below:

Accept: Means that the connection will be authorized to pass through the firewall.

Reject: Means that the connection will not be authorized to pass through the firewall and a *Reset packet* will be sent to the origin host.

Discard: Means that the connection will not pass through the firewall, but no packet will be sent to the origin host.

Repipes: Indicates that the connection will be accepted (but with a different priority that will be specified in the **PIPE** column).

Blocks source: Indicates the host that has originated the connection must to be blocked for some time (it means, all connections originated from this host will be rejected). The column **Block Timeout** is used to specify how long this host will remain blocked.

Pipe: This column is enabled only if the action **Repipe** has been selected. It indicates the new priority that will be assigned to the connection. An entity of type pipe (for more information see the chapter **Registering entities**)

Block Timeout: This column will be enabled only if the action **Blocks Source** has been selected. It indicates how long the host will remain blocked.

34.3. Creating application filters

The Application Filters inform the firewall what need to be searched in a communication, to make possible the identification of a specific protocol or file type. The product already come with several preconfigured filters, however is possible that the administrator configure new filters to meet his needs.

To gain access to the Application filters creation window follow the steps below:

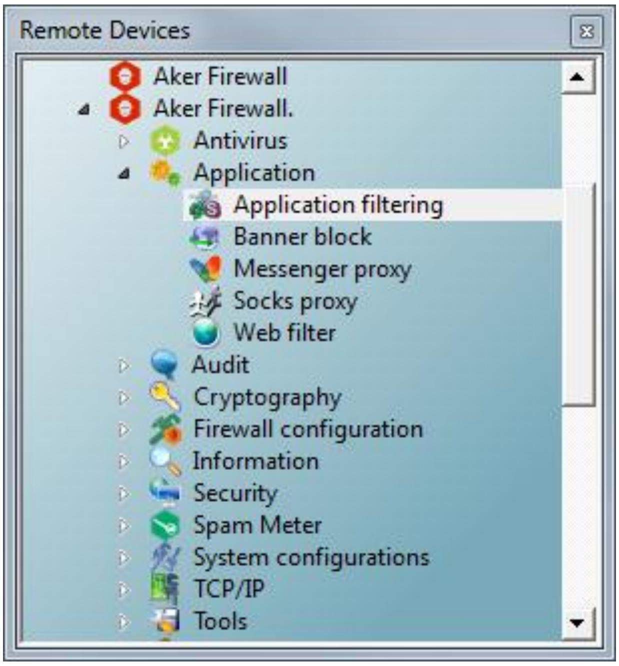
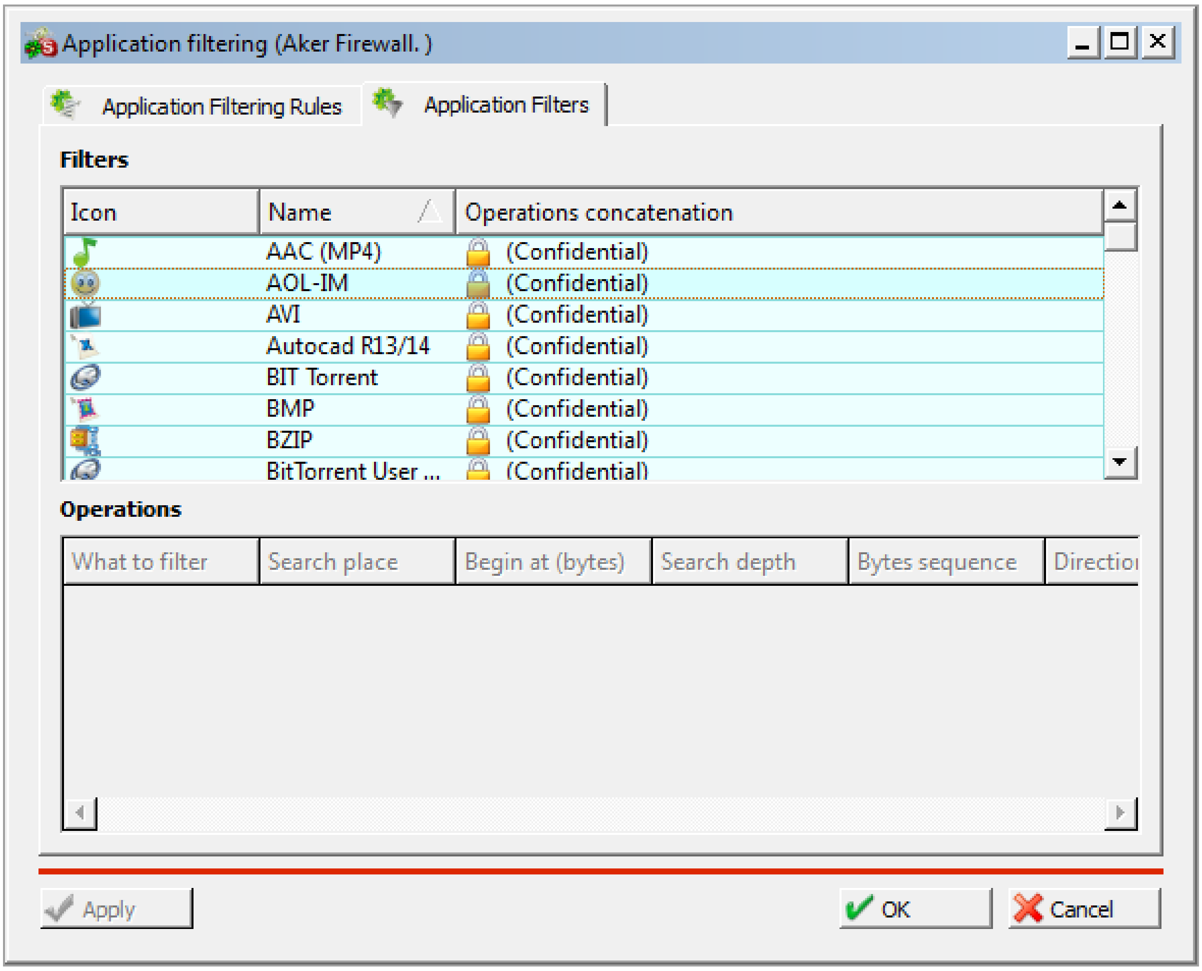

Remote Devices
Aker Firewall
Aker Firewall.
Antivirus
Application
Application filtering
Banner block
Messenger proxy
Socks proxy
Web filter
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 495 – Access window: Application filtering.

- Click on the *Application* menu.
- Select *Application filtering*.
- Then select the *Application filter tab*.

Application


Application filtering (Aker Firewall.)
Application Filtering Rules
Application Filters
Apply
OK
Cancel

Filters

Icon	Name	Operations concatenation
	AAC (MP4)	(Confidential)
	AOL-IM	(Confidential)
	AVI	(Confidential)
	Autocad R13/14	(Confidential)
	BIT Torrent	(Confidential)
	BMP	(Confidential)
	BZIP	(Confidential)
	BitTorrent User ...	(Confidential)

Operations

What to filter	Search place	Begin at (bytes)	Search depth	Bytes sequence	Directio

Image 496 – Application Filters

This window is divided into two parts. At top there is a list of filters recently created. Selecting a filter, will be displayed at the bottom part the search operation related to the filter you have selected.

Below follows the operation options menu for the *Application Filter rules*

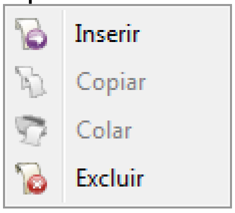

Inserir
Copiar
Colar
Excluir

Image 497 – Option menu.

- **Insert:** Adds a new rule.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes a rule you have recently copied to the list.
- **Delete**: Deletes the selected rule.

To change a filter's name or edit it, simply right-click on it, and them the following options will be displayed:

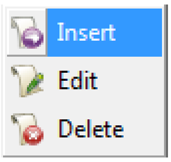
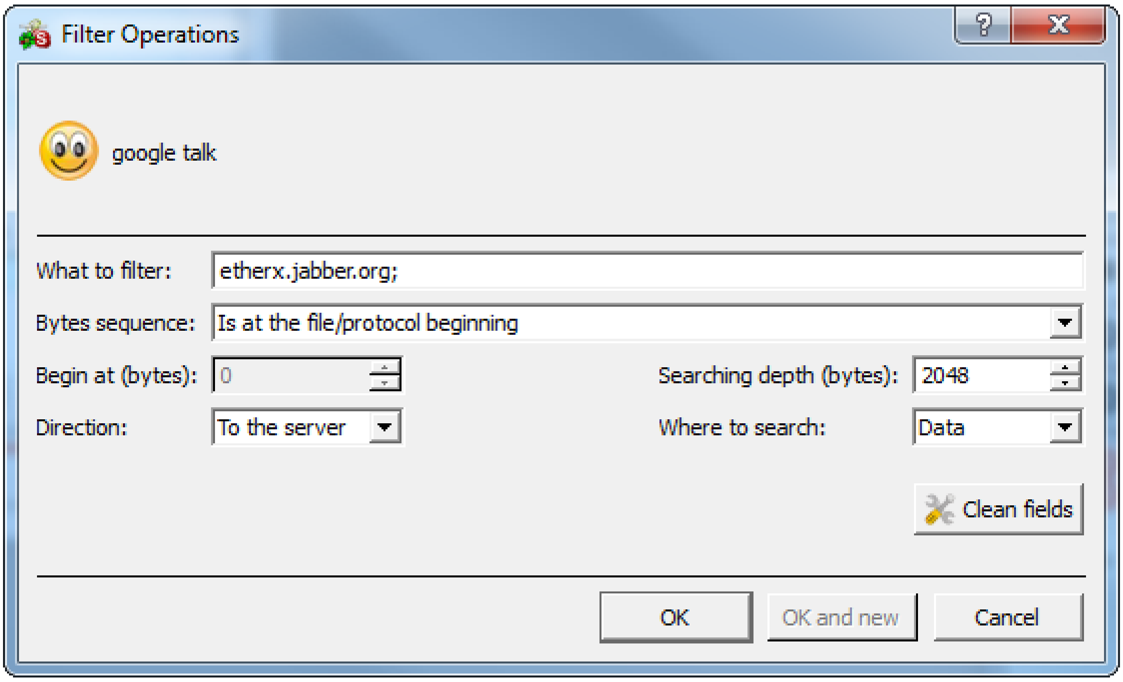


Image 498 – option menu.

- **Insert:** Adds a new operation for the selected filter.
- **Edit** Opens the window below, to make any change in the operation.
- **Delete:** Removes the selected operation from the list.

When editing an operation the following window will be displayed:



google talk

What to filter: etherx.jabber.org;

Bytes sequence: Is at the file/protocol beginning

Begin at (bytes): 0

Searching depth (bytes): 2048

Direction: To the server

Where to search: Data

Image 499 – Filter Operations

What to filter: In this field shall be added the sequence of bytes that will be searched in the connection.

Byte sequence: Defines the sequence of data that will be searched in the file/protocol data or in the metadata (header).

Begin at (bytes): In case you have chosen the search will be done from the middle of the file or communication, this field is used to specify the position that the search shall begin.

Direction: Direction that the data will be analyzed to verify the existence of the sequence that has been set in the "**What to Filter"** field.

Searching depth (bytes): This field indicates the amount of bytes that will be analyzed dynamically from the beginning of the search.

Where to search: This filed specifies if the search will start from the beginning of the file/communication or any other point.

Configuring the IDS/IPS

35. Configuring the IDS/IPS

This chapter shows the functions provided by the IPS/IDS set and how to perform its configuration.

About IPS/IDS module

Aker Firewall's IPS/IDS module brings together several functions to identify and block cyber-attacks in real time. This module works together with the firewall in order to provide high degree of protection to your network. The internal module has several preconfigured attacks that can be updated on the Internet. Besides the internal module, you can use the external IDS as well in order to gain an even higher degree of protection.

35.1. Accessing the IPS/IDS

To gain access to the IPS/IDS configuration window, follow the steps below:

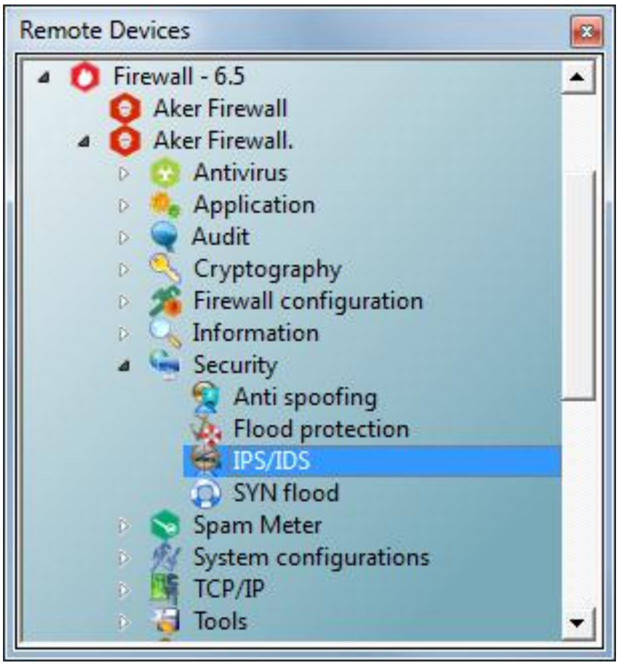

Remote Devices
Firewall - 6.5
Aker Firewall
Aker Firewall.
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Anti spoofing
Flood protection
IPS/IDS
SYN flood
Spam Meter
System configurations
TCP/IP
Tools

Image 500 – Access window: IPS/IDS.

- Click on the Security menu.

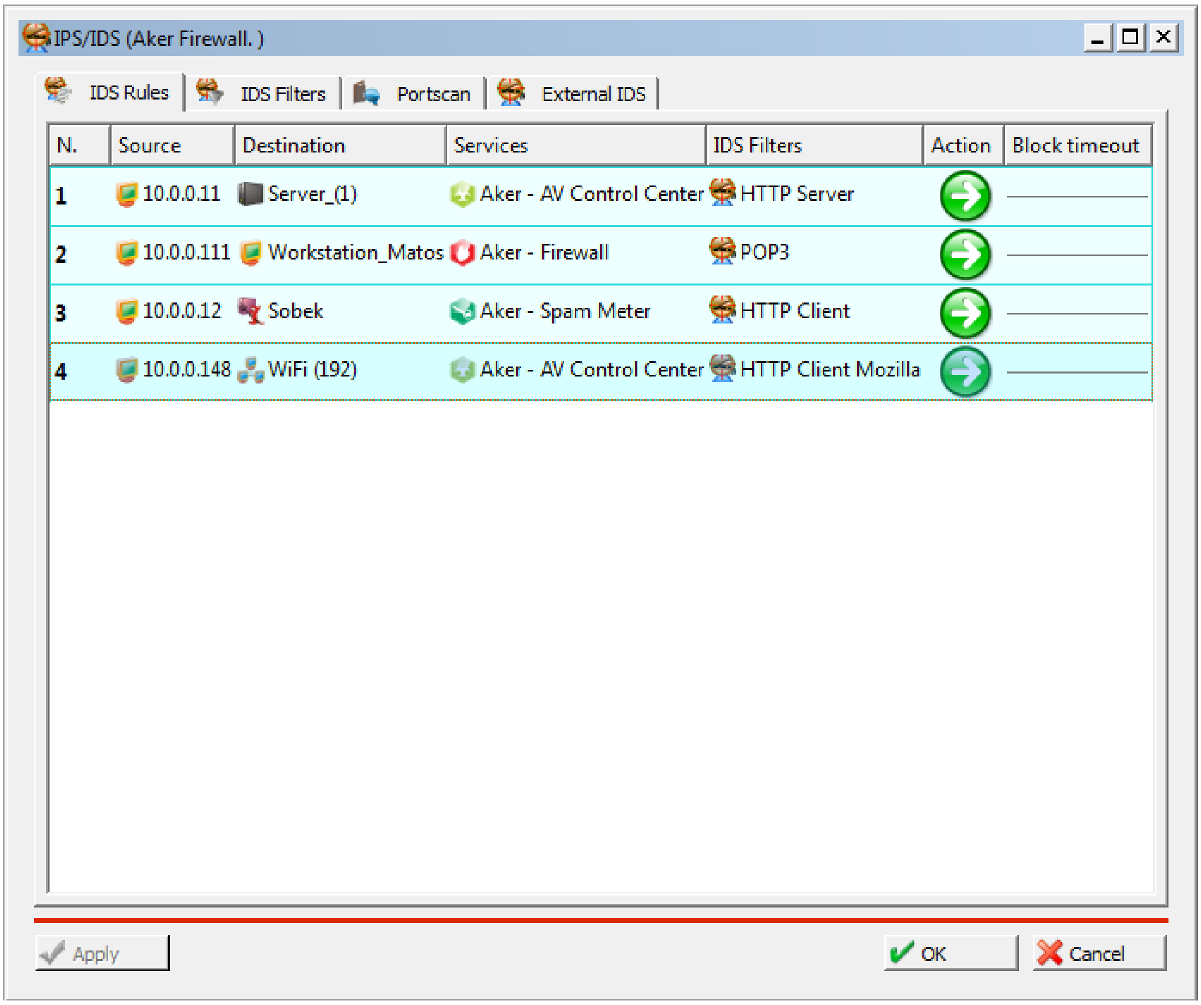
- Select *IPS/IDS.*

IDS/IPS configuration window

This window has for tabs that are responsible for the IDS module configuration.

- The **OK** button will close window saving all changes.
- The **Apply** button will save all changes and keep the window opened.
- The **Cancel** button will discard all changes closing the window.

IDS rules



N.	Source	Destination	Services	IDS Filters	Action	Block timeout
1	10.0.0.11	Server_(1)	Aker - AV Control Center	HTTP Server	→	—
2	10.0.0.111	Workstation_Matos	Aker - Firewall	POP3	→	—
3	10.0.0.12	Sobek	Aker - Spam Meter	HTTP Client	→	—
4	10.0.0.148	WiFi (192)	Aker - AV Control Center	HTTP Client Mozilla	→	—

Image 501 – IPS/IDS – IDS rules.

This tab has all IDS rules defined in Aker Firewall, each rule is displayed in a separated line.

Below follows the operation options menu for the IDS rules:

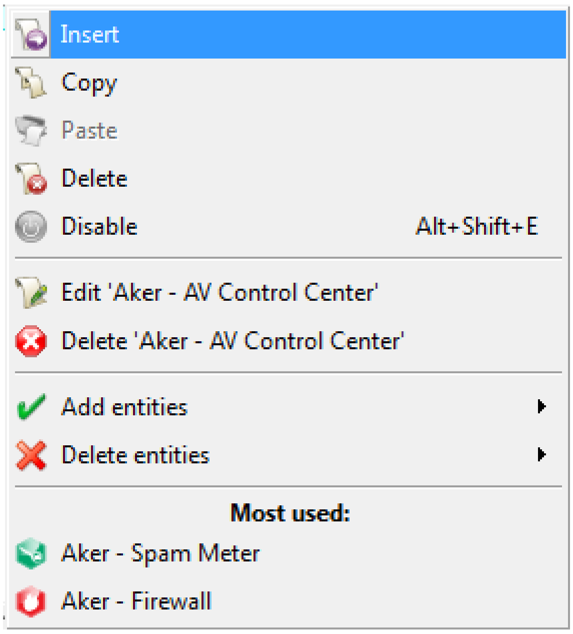

Insert
Copy
Paste
Delete
Disable Alt+Shift+E
Edit 'Aker - AV Control Center'
Delete 'Aker - AV Control Center'
Add entities
Delete entities
Most used:
Aker - Spam Meter
Aker - Firewall

Image 502 – Option menu.

- **Insert:** Adds a new rule.
- **Copy:** Copies the selected rule.
- **Paste:** Pastes a rule you have recently copied to the list.
- **Delete**: Deletes the selected rule.
- **Enable/Disable:** Enables/disables the selected rule.

Each rule consists of the following fields:

Source: Specifies the communications origins that the filter will be inspecting, to do it one or more entities of type: *machine, network, or set* need to be added (for more information see the chapter titled **Registering entities**).

Destination: Specifies the communication destination that the filter will be inspecting, to do it one or more entities of type: *machine, Network, or set* need to be added (for more information see the chapter titled **Registering entities**).

Services: Specifies the communication service that the filter will be inspecting, to do it one or more entities of type *machine* need to be added (for more information see the chapter titled **Registering entities**).

IDS Filters: In this column shall be added the IDS filters that will be active for this communication. One of the available groups of filters need to selected, and after if desired enable the filters inside each group individually.

The available groups are:

- **FTP**: It is composed of filters against attacks targeting FTP server.
- **HTTP**: It is composed of filters against attacks targeting WEB server.
- **HTTP Client**: It is composed of filters against attacks targeting browser.
- **POP3**: It is composed of filters against attacks targeting email readers.

- **IMAP**: It is composed of filters against attacks targeting email readers (IMAP is better than POP3).
- **SMTP**: It is composed of filters against attacks targeting email server.
- **TCP**: It is composed of filters against generic attacks using TCP protocol.
- **UDP**: It is composed of filters against generic attacks using UDP protocol.

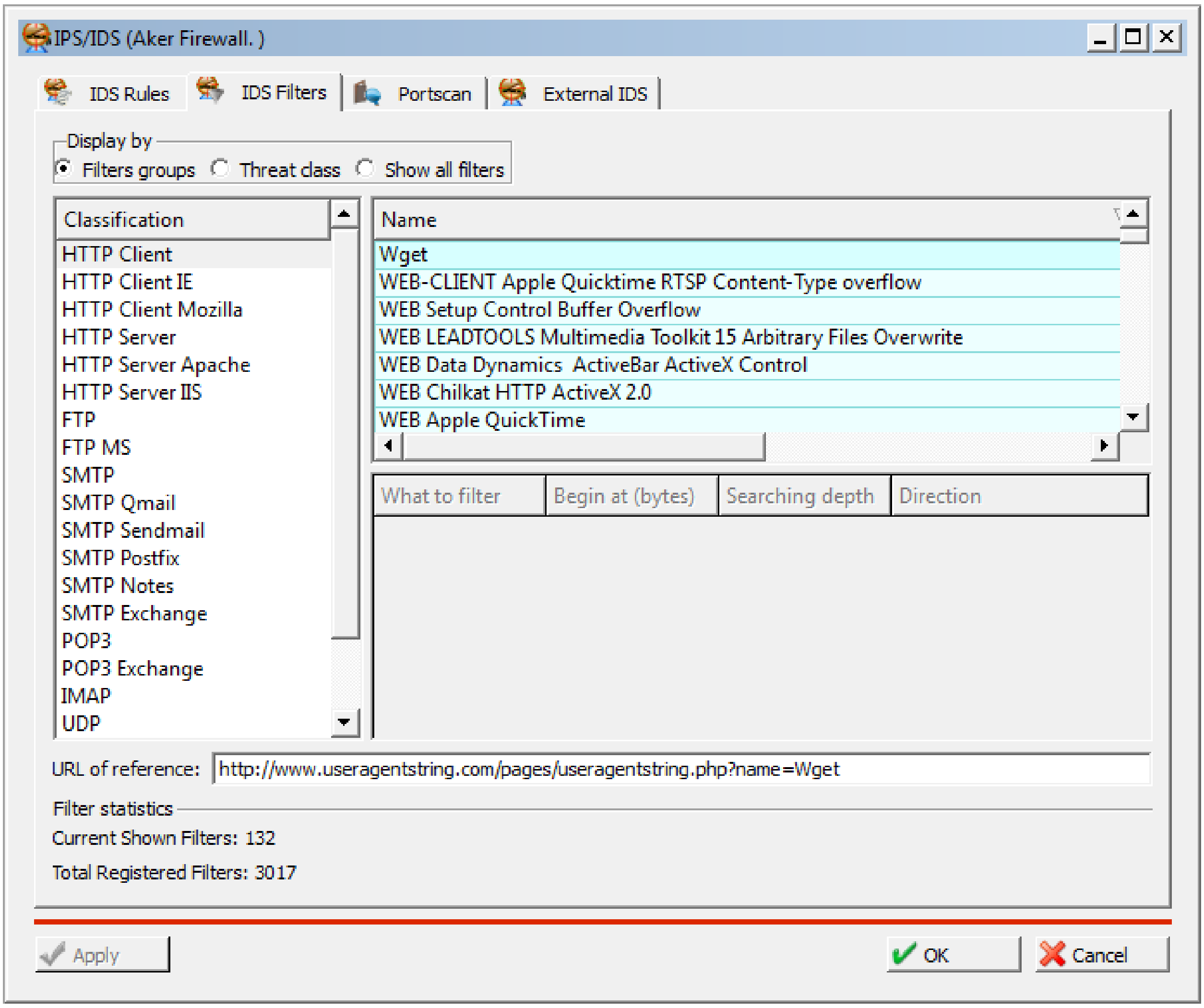
Action: Indicates the action that will be taken by the firewall, in case one of the specified filters is applied. It has two options; the description of them follows below:

Ignore: It means that the attack will be ignored by the firewall.

Block: Indicates the host that has originated the connection must to be blocked for some time (it means, all connections originated from this host will be rejected).

Block timeout: This column indicates how long the attacker will remain blocked.

IDS Filters



Display by
● Filters groups ○ Threat class ○ Show all filters

Classification
HTTP Client
HTTP Client IE
HTTP Client Mozilla
HTTP Server
HTTP Server Apache
HTTP Server IIS
FTP
FTP MS
SMTP
SMTP Qmail
SMTP Sendmail
SMTP Postfix
SMTP Notes
SMTP Exchange
POP3
POP3 Exchange
IMAP
UDP

Name
Wget
WEB-CLIENT Apple Quicktime RTSP Content-Type overflow
WEB Setup Control Buffer Overflow
WEB LEADTOOLS Multimedia Toolkit 15 Arbitrary Files Overwrite
WEB Data Dynamics ActiveBar ActiveX Control
WEB Chilkat HTTP ActiveX 2.0
WEB Apple QuickTime

URL of reference: http://www.useragentstring.com/pages/useragentstring.php?name=Wget

Filter statistics
Current Shown Filters: 132
Total Registered Filters: 3017

Image 503 – IPD/IDS (IDS filters)

This window is used to see the IDS filters that are available in the firewall, and they are also used to create new filters. It consists of a list with all filters that have been created **recently**. There are three different ways to see these filters: by group, by class threat or a list.

Class treats:

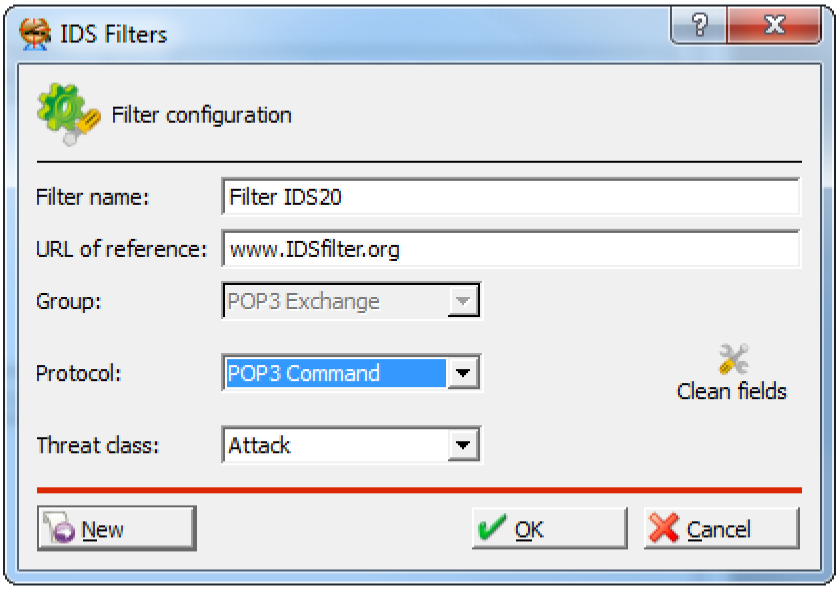
- **Attack**: direct attacks that explore application or operating system’s bugs or vulnerabilities.
- **Malware**: attacks originated from viruses or Trojans.
- **Probe**: port scanning or vulnerability identification.

Filters groups:

- **FTP**: It is composed of filters against attacks targeting FTP servers.
- **HTTP**: It is composed of filters against attacks targeting WEB servers.
- **HTTP Client**: It is composed of filters against attacks targeting browsers.
- **POP3**: It is composed of filters against attacks targeting email readers.
- **SMTP**: It is composed of filters against attacks targeting email servers.
- **TCP**: It is composed of filters against generic attacks using TCP protocol.
- **UDP**: It is composed of filters against generic attacks using UDP protocol.

When selecting a filter, a URL of reference will be displayed allowing the administrator gathers more information about the attack.

To add a new filter, right-click on the list of filters and select the option **“New filter”**:



Filter name: Filter IDS20
URL of reference: www.IDSfilter.org
Group: POP3 Exchange
Protocol: POP3 Command
Threat class: Attack

Image 504 – IDS Filter – Filter configuration.

Edition/ creation of filters

- The **OK** button will close window saving all changes.
- The **Apply** button will save all changes and keep the window opened.
- The **Cancel** button will discard all changes closing the window.

This window allows creating a new filter or change filter’s parameters that already exists. This window consists of the following fields:

Filter name: Name which the filter will be known by the firewall.

URL of reference: URL that allows the administrator gathers more information about the attack.

What to filter: In this field shall be added the sequence of bytes that will identify the attack.

Begin at: This field is used to identify the position that the data flow need to begin the search at.

Searching depth (bytes): This field indicates the amount of bytes that will be analyzed dynamically from the beginning of the search.

Direction: Direction that the data will be analyzed to verify the existence of the sequence that has been set in the "**What to Filter"** field.

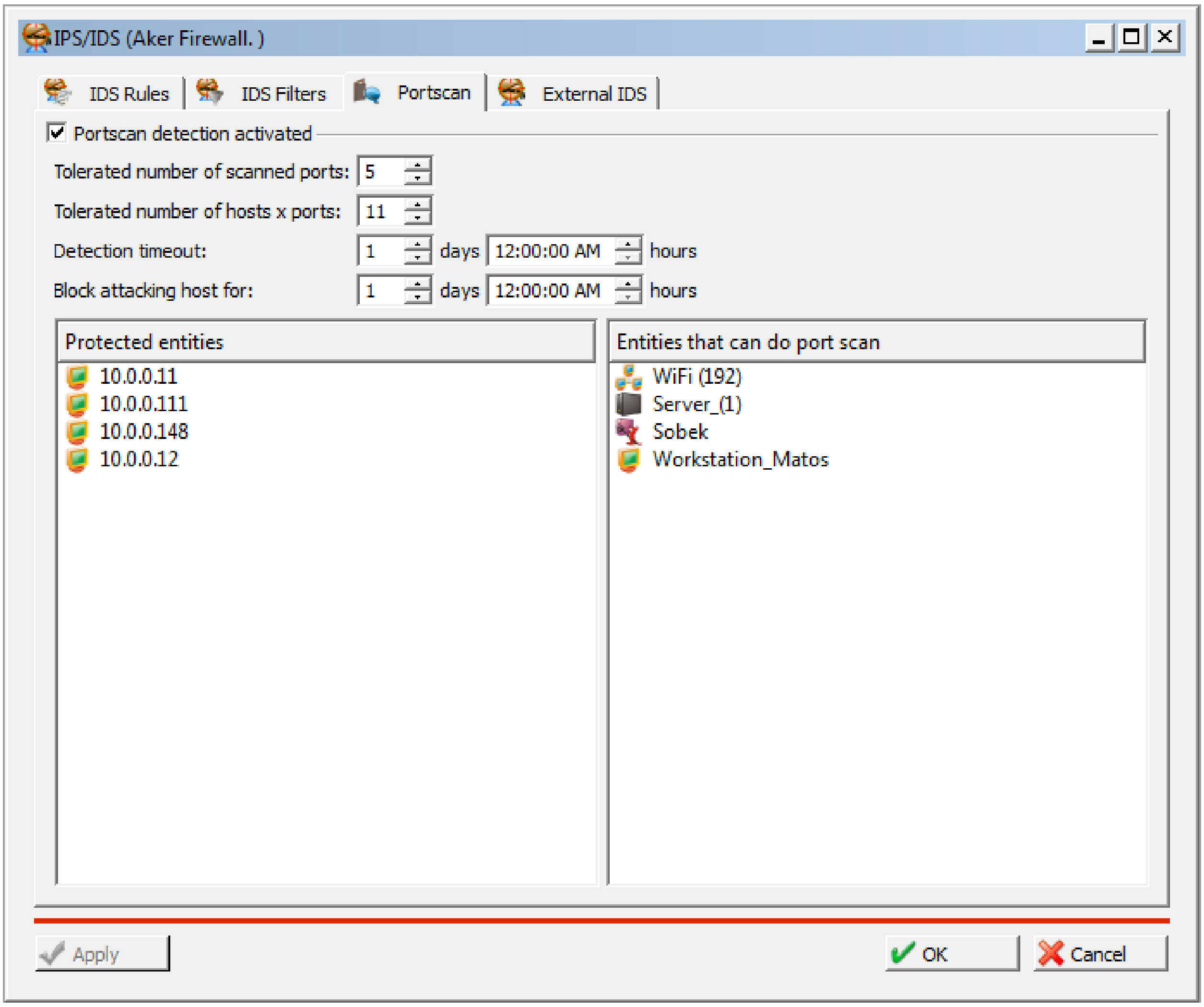
Protocol: indicates which protocol the attack will be searched. The available options are:

- **UDP:** Search data directly in the UDP protocol.
- **TCP** Search data directly in the TCP protocol.
- **HTTP header:** Search data in the HTTP protocol header.
- **URL HTTP:** Search data in the HTTP protocol URLs.
- **HTTP body:** Search data in the HTTP protocol body.
- **SMTP command:** Search data in the SMTP protocol commands.
- **SMTP body:** Search data in the SMTP protocol body.
- **FTP command:** Search data in the FTP protocol commands.
- **FTP data:** Search data in the FTP protocol body.
- **POP3 command:** Search data in the POP3 protocol commands.
- **POP3 data:** Search data in the POP3 protocol body.

Group: This field informs the firewall which *group* the attack shall be placed at.

Threat class: This field informs the firewall which *threat class* the attack shall be placed at.

Portscan



☑ Portscan detection activated

Tolerated number of scanned ports: 5

Tolerated number of hosts x ports: 11

Detection timeout: 1 days 12:00:00 AM hours

Block attacking host for: 1 days 12:00:00 AM hours

Protected entities	Entities that can do port scan
10.0.0.11	WiFi (192)
10.0.0.111	Server_(1)
10.0.0.148	Sobek
10.0.0.12	Workstation_Matos

Image 505 – IPD/IDS – Portscan.

This tab is used to configure the protection against “*Port Scanning Attacks*”. These attacks attempt to access all or several communication ports in one or more hosts of a network.

To configure the protection against *“Port Scanning Attacks”*, the following fields need to be filled in:

Portscan detection activated: This option need to be selected in order to activate the port scan detection support.

Tolerated number of scanned ports: This field indicates the maximum number of ports that can be accessed in the same host. Accessing a number of ports larger than the number of ports configured in this option will cause the source host blocking.

Tolerated number of hosts x ports: This field indicates the maximum number of ports that can be accessed in one or more hosts. It would be like an attacker attempt to access two ports in one host or a port in two hosts.

Example: If this parameter is 12, any person would access the following combination without it being taken as an attack:

- 12 ports per host in 1 host
- 6 ports per host in 2 host
- 4 ports per host in 3 host
- 3 ports per host in 4 host
- 1 ports per host in 12 host

Detection timeout: This field indicates the time that the information of access will be kept by the firewall. Low values will make the port scan be very slow (e.g. 1 port per 1 hour). High values will occupy unnecessary memory.

Block attacking host for: In case detecting a port scan attack, this column indicates how long the host attacker will remain blocked, disabling the start of a connection through the firewall.

Protected entities: This list indicates entities such as hosts, networks, or sets that will be protected against port scan attacks.

In order to add a new list, follow the steps below:

- *You can drag-n-drop* entities, from the entity list.
- Right-click and select the option **Insert**, to add a new entity

To remove an entity from the list: selected the entity and hit the key “**DELETE**” on your keyboard, or right-click on the entity you wish to remove, and select **Delete.**

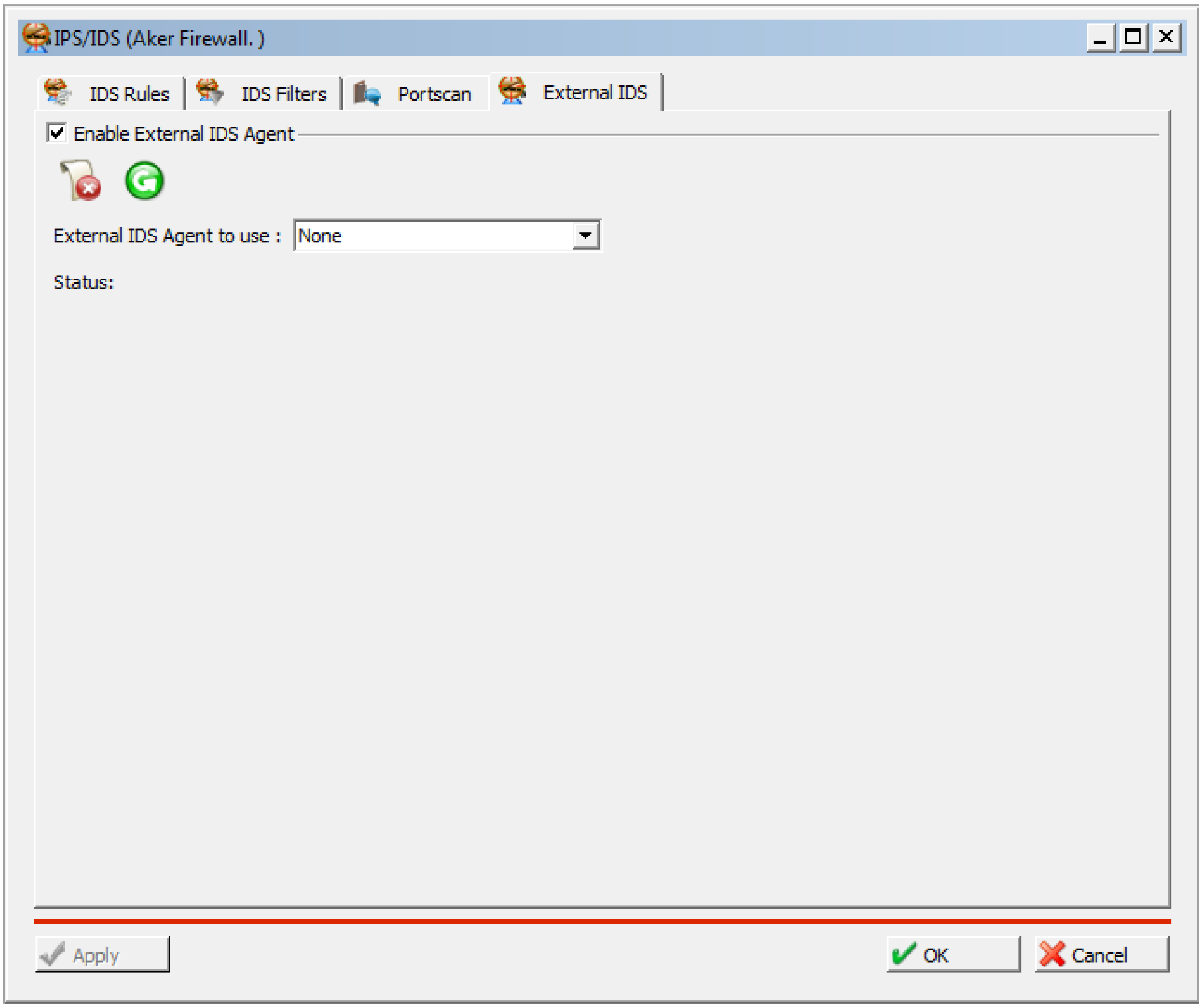
Entities that can do port scan: This list indicates entities such as hosts, networks, or sets that will be protected against port scan attacks. This list is used to release the access to vulnerability detection or monitoring.

In order to add a new list, follow the steps below:

- *You can drag-n-drop* entities, from the entity list.
- Right-click and select the option **Insert**, to add a new entity

To remove an entity from the list: selected the entity and hit the key “**DELETE**” on your keyboard, or right-click on the entity you wish to remove, and select **Delete**.

External IDS



☑ Enable External IDS Agent

External IDS Agent to use : None

Status:

Image 506 – IPD/IDS – External IDS.

This window configures all parameters that allow IDS agents to add the blocking rules to the firewall.

- The **OK** button will close the IDS agent configuration window, and save all changes.
- The **Cancel** button will close the window but will not apply any modification.
- The **Apply** button will send all changes to the firewall, and will keep the window open.

Parameter meaning

Enable IDS Agent: This option must be checked to activate IDS agent support, and unchecked to deactivate it. (When IDS agent support is disabled, old configurations remain stored, but cannot be altered).

IDS Agent to use: Indicates the IDS agent enabled to add blocking rules to the firewall. This agent must have been previously registered in the firewall. For more information, see the chapter titled **Registering Entities chapter**.

Status: Allows the administrator to verify the status of the connection to the IDS agent. A green value, with the word *Connected*, indicates that the firewall was successfully authenticated and the communication with the agent was established.

The **Check IDS connection status** button will refresh the connection status.

The **Flush the IDS rules** button will exclude from the firewall all rules registered by the IDS agent.

35.2. View blocked IPs

It is possible to view the list of IP that is blocked in the firewall, due to the inclusion IDS/IPS module temporary block rule.

To gain access to the Blocked IPs window follow the steps below:

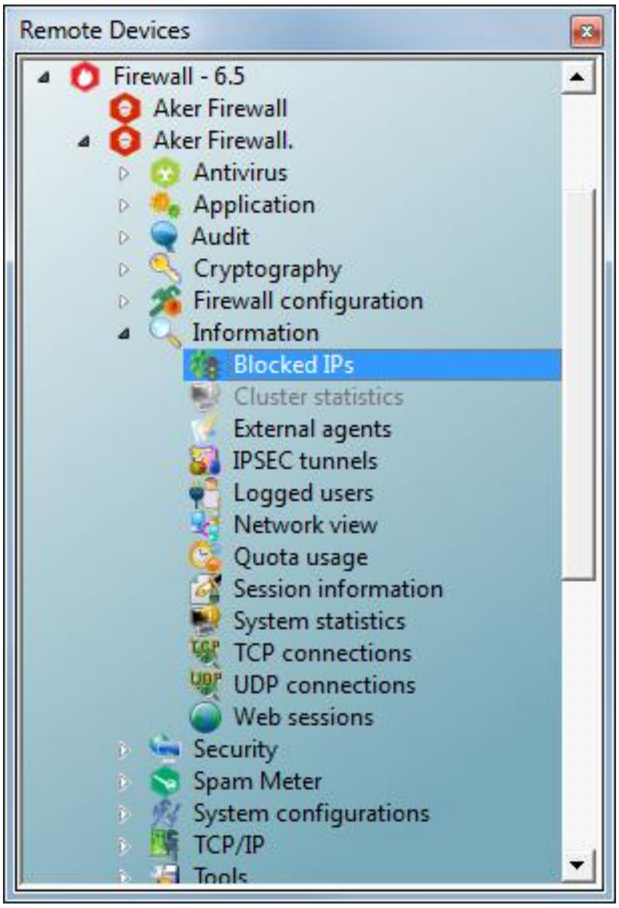

Remote Devices
Firewall - 6.5
Aker Firewall
Aker Firewall.
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 507 – Access window: Blocked IPs

- Click on the *Information* menu.
- Select *Blocked IPs.*

Blocked IPs window

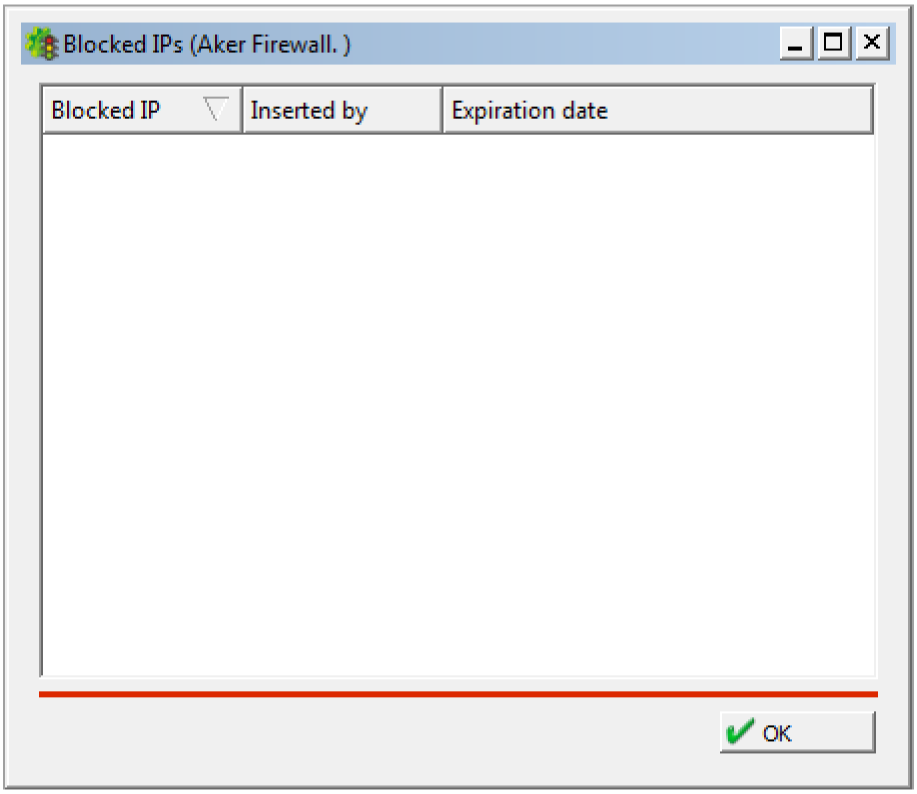

Blocked IPs (Aker Firewall.)
Blocked IP
Inserted by
Expiration date
OK

Image 508 – Blocked IPs

This window consists of a list where each blocked IP is displayed in a line with the following information:

Blocked IP: IP address of host that has been blocked;

Inserted by: Module that has inserted the temporary blocking rule;

Expiration date: sets the date which the IP will remain blocked;

To remove an IP from the list, simply right-click, and select the ***Delete IP*** option**;**

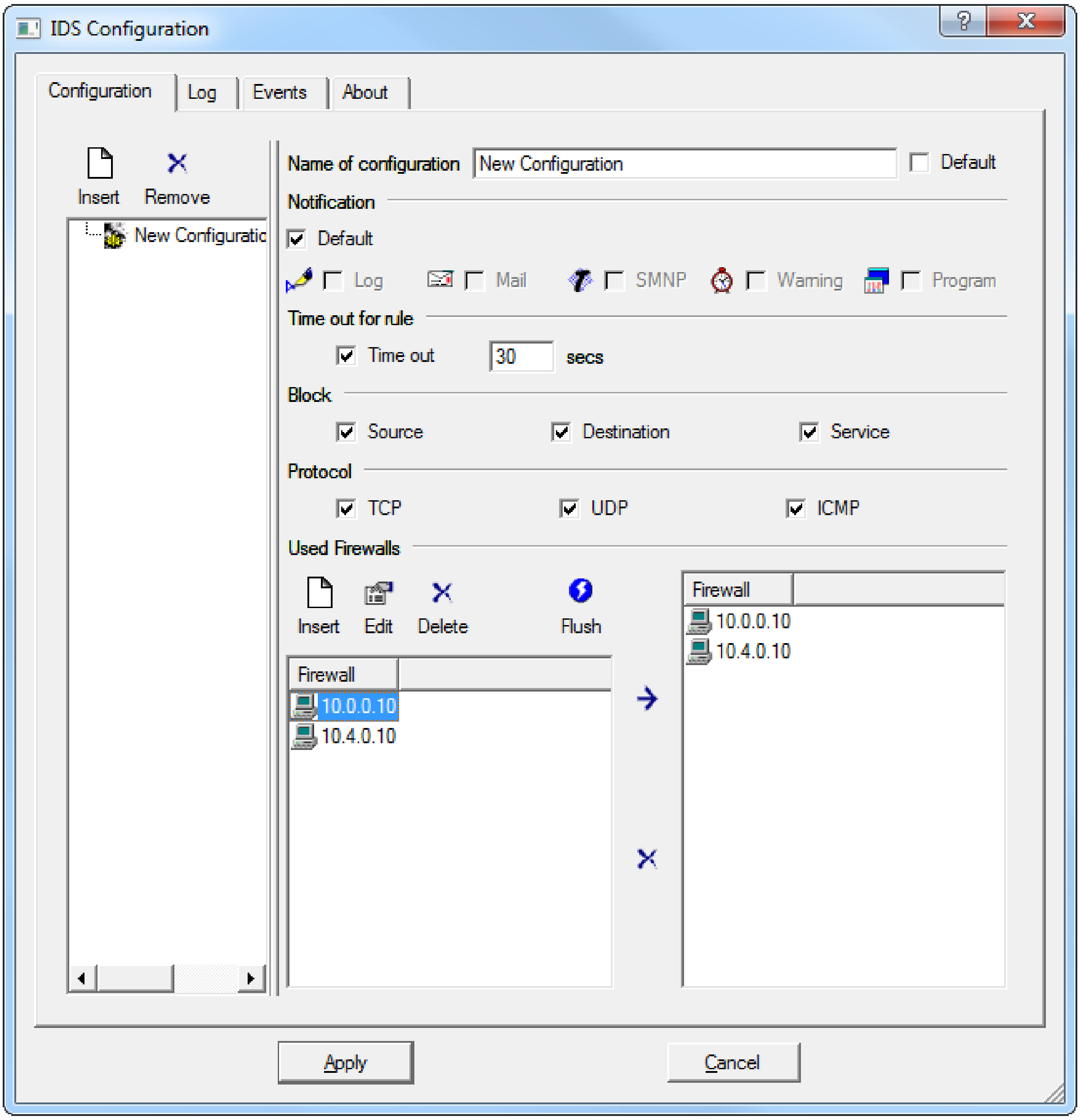
35.3. Installing IDS External Plugin on Windows

In order to use the External IDS, besides the configuration displayed in **External IDS**, it is required to install a plugin to make possible the communication between the external IDS and the firewall. This plugin's installation is very simple, and its download is made at Aker's website (http://www.aker.com.br).

Aker Firewall plugin configuration for External IDS

After the plugin installation, it is necessary to configure it. This configuration allows registration of all firewalls that will be notified, as well as the definition of the rules that will be added.

To access the configuration program, click on the *Start* menu, and select *Aker Firewall* group. Inside it, select the *Intrusion Detection* group, and then, the *Intrusion Detection* option. The following window will be displayed:


IDS Configuration
Configuration
Log
Events
About
Insert
Remove
New Configuratio
Insert
Edit
Delete
Flush
Apply
Cancel

Name of configuration: New Configuration ☐ Default

Notification

☑ Default

☐ Log ☐ Mail ☐ SMNP ☐ Warning ☐ Program

Time out for rule

☑ Time out 30 secs

Block

☑ Source ☑ Destination ☑ Service

Protocol

☑ TCP ☑ UDP ☑ ICMP

Used Firewalls

Firewall
10.0.0.10
10.4.0.10

Firewall
10.0.0.10
10.4.0.10

Image 511 – IDS configuration (configuration tab)

This window has 4 tabs. In the first one, displayed above, is where the plugin configuration is done. It has a list with the names of the several configurations created by the administrator, and that will later be displayed as action options in the Real Secure administration console. It is possible to specify a configuration name when an event is being executed, or to use the **Default** button to specify a configuration that will be executed by default, i.e., when no configuration name is specified.

To create a new configuration, click on the **Insert** button, located in the top left side of the window. A blank configuration will be created. To edit a configuration parameter, click on its name, and modify the desired parameters.

Parameter meaning

Name of configuration: The name that will be displayed in the administration consoles of Real Secure™, NFRTM, Enterasys Dragon, and Snort. When selected, it will execute the actions defined by the administrator.

Notification: This field allows definition of the actions that will be executed by the firewall, when a blocking rule is added through the execution of a configuration. If the **Default** option is selected, the actions associated to the message “IDS blocking rule added” will be executed. Otherwise, it is possible to specify exactly the actions to be taken. For more information on action configuration, see the chapter titled **Configuring System Actions**.

Block: This field is used to define the type of blocking that will be performed when the configuration is executed. There are three possible options that may be independently selected (when more than one option is selected, the rule will block packets that match all, and not just some, checked options):

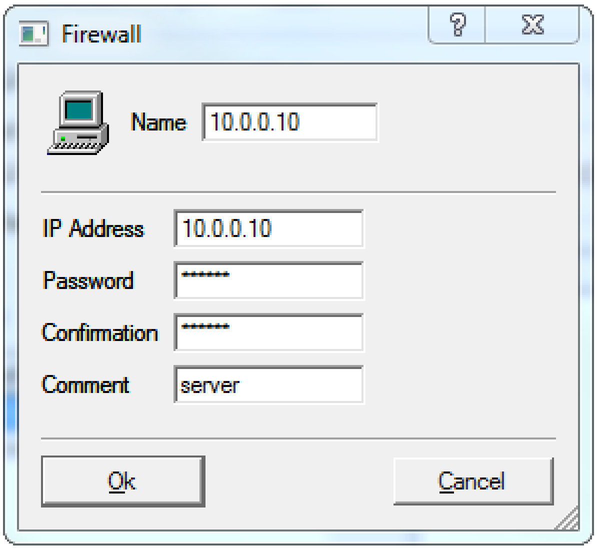
Source: Packets with source addresses equal to the rule’s packets will be blocked.

Destination: Packets with destination addresses equal to the rule’s packets will be blocked.

Service: Packets using the same service as the rule will be blocked. If this option is checked, the protocols that will be associated to the service must be selected in the **Protocol** field. This is necessary because Real Secure™ has a limitation. It does not supply the protocol of a service, only its number. Since NFR only inspects TCP traffic, this protocol must be selected when this IDS is being used.

Time out for rule: This field is used to define how long the rules added by the configuration will remain active. If the option **Activation Time** is checked, this must be specified, in seconds. If this option is unchecked, the rule will remain active until next time the firewall is restarted.

Used Firewalls: This field defines which firewalls the temporary rules will be added. An access password and IP address must be configured for each firewall. The access password must be the same configured in the definition of the IDS agent entity (for more information, see the chapter titled **Registering Entities chapter**). When the Insert or Edit buttons are pressed, the following window will show up:



Name 10.0.0.10

IP Address 10.0.0.10

Password ******

Confirmation ******

Comment server

Image 512 – Used firewalls

The firewalls defined above, must be added to the configuration through the following steps:

Select the required firewalls; press the arrow button so that the selected firewalls will show up on the right list of the window.

The **Flush** button deletes the dynamic rules added to the selected firewalls by the IDS.

After all modifications are done, click on the **Apply** button. If the Real Secure is being used, a window will show up saying that the Real Secure Global Responses will be modified, and asking for a confirmation to continue. Click on the **Yes** button, to save the new configuration.

Log

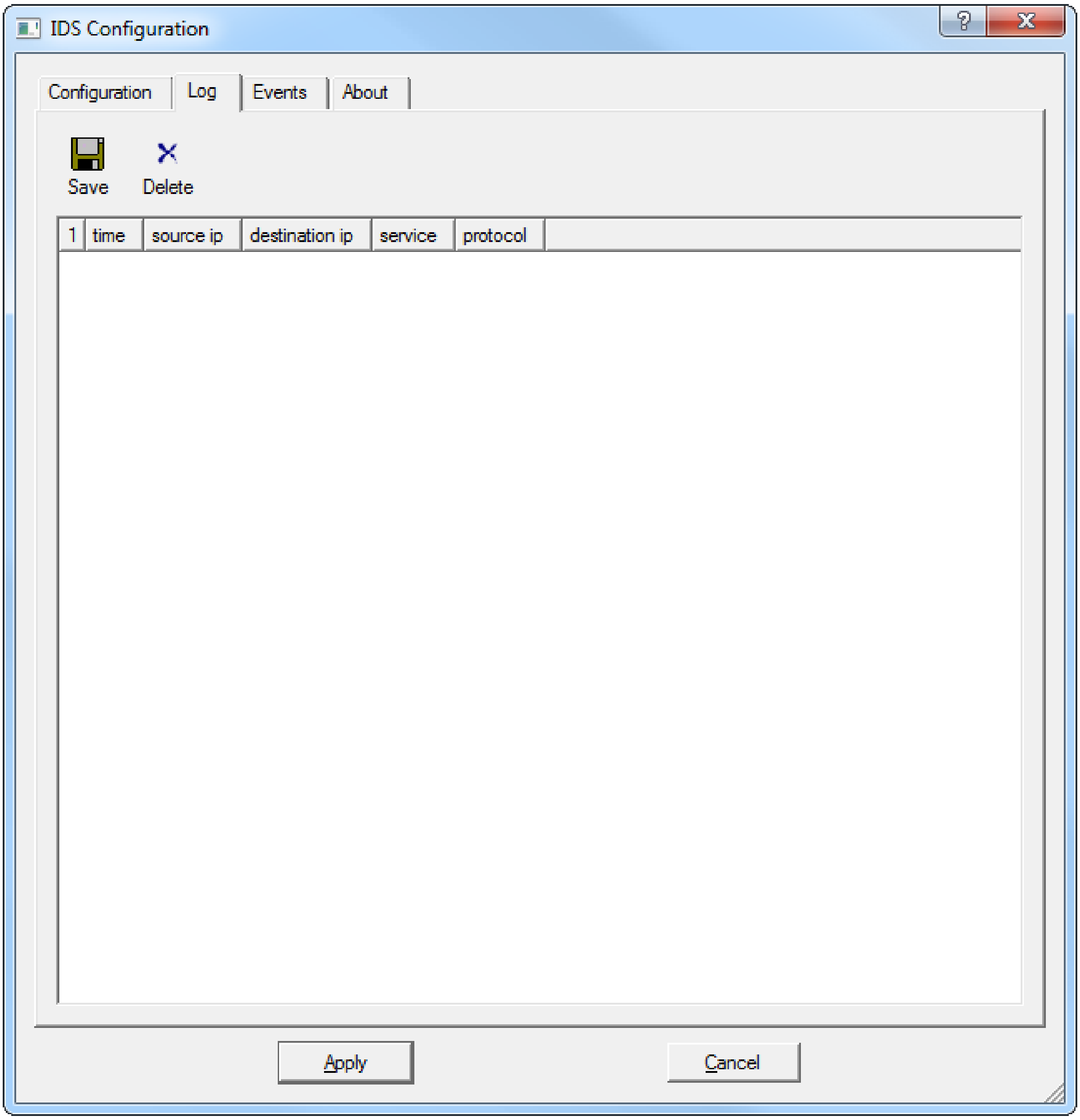
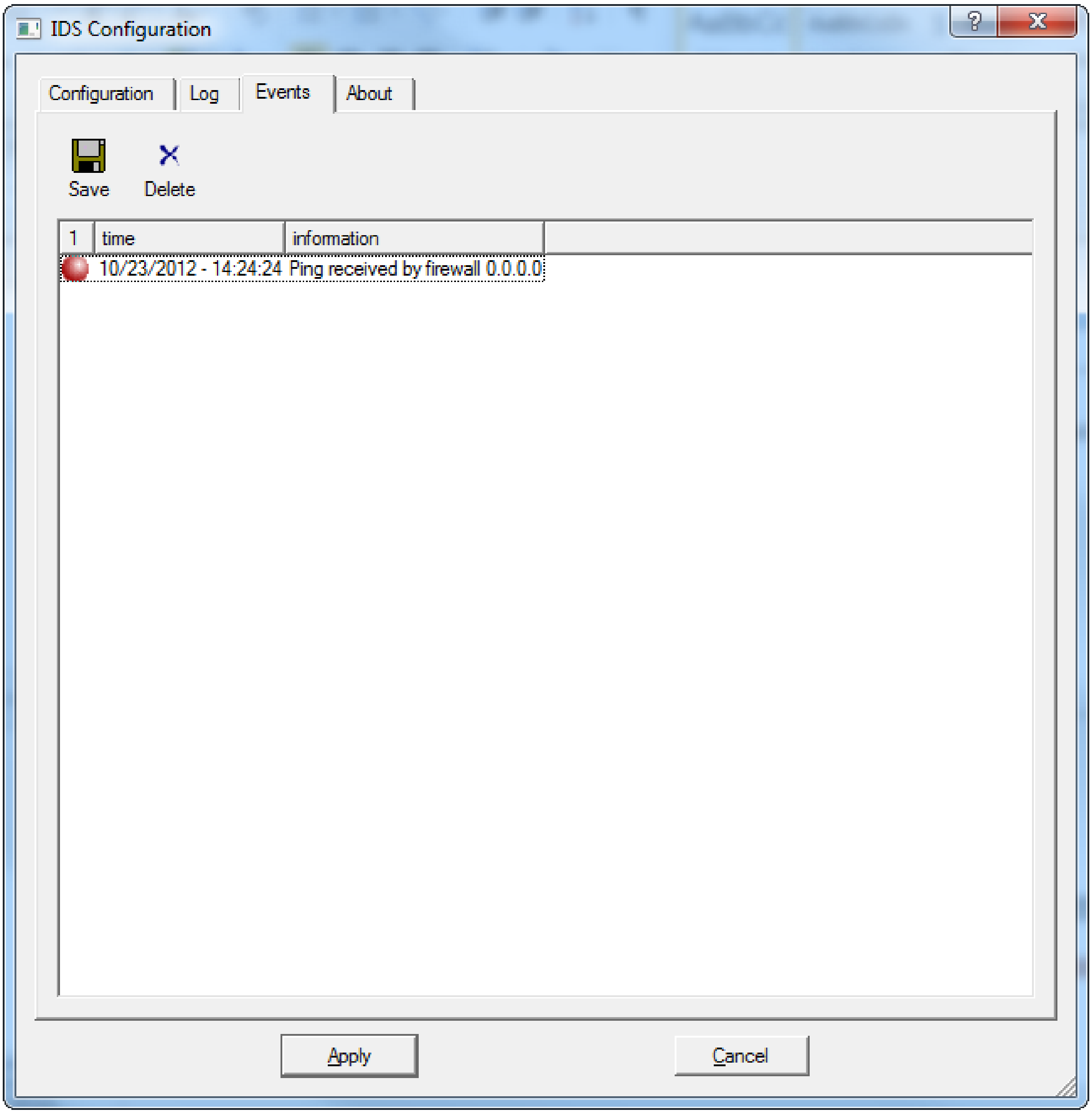

IDS Configuration
Configuration
Log
Events
About
Save
Delete
1
time
source ip
destination ip
service
protocol
Apply
Cancel

Image 513 – IDS configuration – log tab

All blocks sent by the IDS will be configured in this window.

Events


IDS Configuration
Configuration
Log
Events
About
Save
Delete
Apply
Cancel

1	time	information
●	10/23/2012 - 14:24:24	Ping received by firewall 0.0.0.0

Image 514 – IDS configuration – events

This is a very useful tab to track agent operation. It has a list of several messages in chronological order. Next to each message, there is a colored icon symbolizing its priority.

35.4. Using the Text Interface – Portscan

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command "fwshell" before you take any action*).

Program location: /aker/bin/firewall/fwportscan

Syntax:

```
fwportscan [help | show | activate | deactivate]
fwportscan [max_ports | max_access] <number>
fwportscan [time_detection | time_block] <time in seconds>
fwportscan [add | remove] protected <entity>
fwportscan [add | remove] authorized <entity>
```

Program help:

```
fwportscan – Configure Portscan parameters
Usage: fwportscan [help | show | activate | deactivate]

show = shows current settings

activate = activates protection against portscan.

deactivate = deactivates protection against portscan.

max_ports = sets the maximum number of ports that can be accessed by a host in
the same server, not taking it as portscan.

max_access = sets the maximum number of distinct access.

ports that can be accessed by a host, which is not taken as portscan.

time_detection = sets the time in seconds that an access done by a host will not be
accounted in future detections against portscan

time_block = sets the time in seconds that a hosts will be blocked after detecting a
portscan.

add = adds a new entity.

delete = removes the selected entity.

help = shows this message.
```

To add or remove we have:

protected = add/delete an entity from the entities list that is protected against portscan.

authorized = add/delete an entity from the entities list that can perform the portscan.

Example 1: (Activating support to portscan detection)

```
#/aker/bin/firewall/fwportscan activate
```

Example 2: (showing protection against portscan current settings)

```
#/aker/bin/firewall/fwportscan show
```

35.5. Using the Text Interface – External IDS

This interface has the same capability as the Remote Interface and it is very simple to be managed *(to use the commands without the FW prefix execute the command “fwshell” before you take any action*).

Program location*: /aker/bin/firewall/fwids*

Sintax*:*

```
        fwids [enable | disable | show | clear | help]
        fwids agent <entity>
        fwids block [source <source ip>] [destination <destination ip>]
                    [service <service/protocol>] [time]
```

Program Help:

```
fwids – Configures IDS external agent parameters
Usage: fwids [enable | disable | show | clear | help]
   fwids agent <entity>
fwids block [source <source ip>] [destination <destination ip>]
            [service <service/protocol>] [time]

    enable      = enables IDS external agents operation
    disable     = disables IDS external agents operation
    show        = shows current configuration
    block       = adds a temporary blocking rule
    clear       = removes all temporary blocking rules
    agent       = specifies name of entity with agent data
    help        = displays this message
```

For the block command, we have:

source = indicates that connections originating in the specified IP address must be blocked

destination = indicates that connections going to the specified IP address must be blocked

service = indicates that connections using specified service must be blocked. In this case, the following must be done:

specify the service as the port for TCP and UDP protocols;
specify the type of service for ICMP;
or
the protocol number for other protocols (ex: 23/tcp, 53/udp, 57/other)

time = time, in seconds, during which the rule will remain active. If not specified, the rule will be active until next time the firewall is started

Example 1: (Enabling support for intrusion detection)

```
#/aker/bin/firewall/fwids enable
```

Example 2: (Setting IDS agent)

```
#/aker/bin/firewall/fwids agent Agent_IDS
```

The entity IDS_Agent must have been previously registered in the system. For more information on how to register entities in Aker Firewall, see the chapter titled Registering Entities.

Exemplo 3: (Showing current configuration)

```
#/aker/bin /firewall/ fwids show

Configuration parameters:

---------------------------

External IDS agent: enabled

Agent: Agent_IDS
```

Example 4: (Adding a blocking rule from host 192.168.0.25 to host 10.0.0.38, in the WWW service, port 80 of TCP protocol, for one hour)

```
#/etc/firewall/fwids block source 192.168.0.25 destination 10.0.0.38 service 80/tcp 3600
```

TCP/IP Settings

36. TCP/IP settings

This chapter shows what is TCP/IP used for and how to configure it in Aker Firewall network.

36.1. TCP/IP settings

This option configures all firewall TCP/IP parameters through the Remote Interface. It is possible to configure network interface addresses, DNS, and basic routing such as PPPoE, 3G and server/relay DHCP.

To gain access to the TCP/IP configuration window follow the steps below:

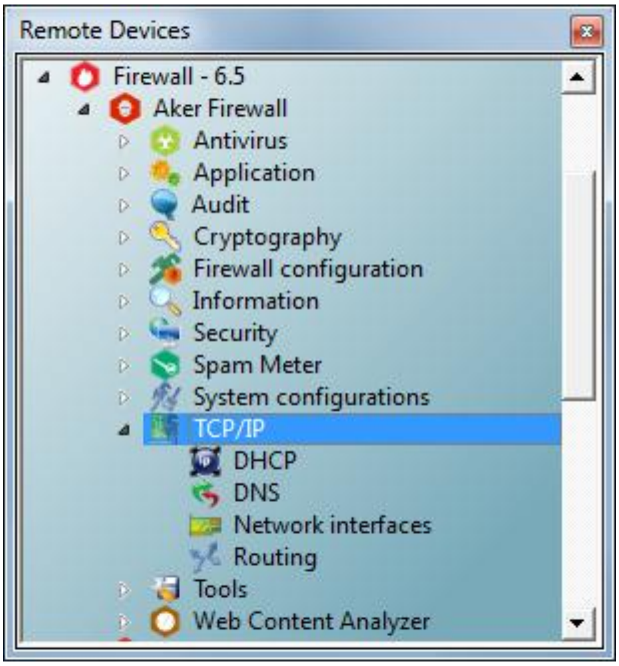

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
DHCP
DNS
Network interfaces
Routing
Tools
Web Content Analyzer

Image 515 – Access window: TCP/IP.

- Click on the TCP/IP menu in the firewall administration

36.2. DHCP

To access the DHCP configuration window follow the steps below:

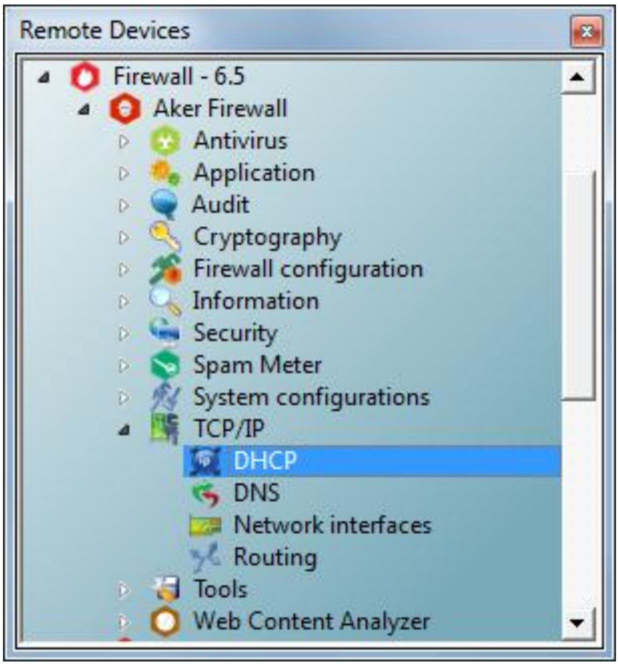
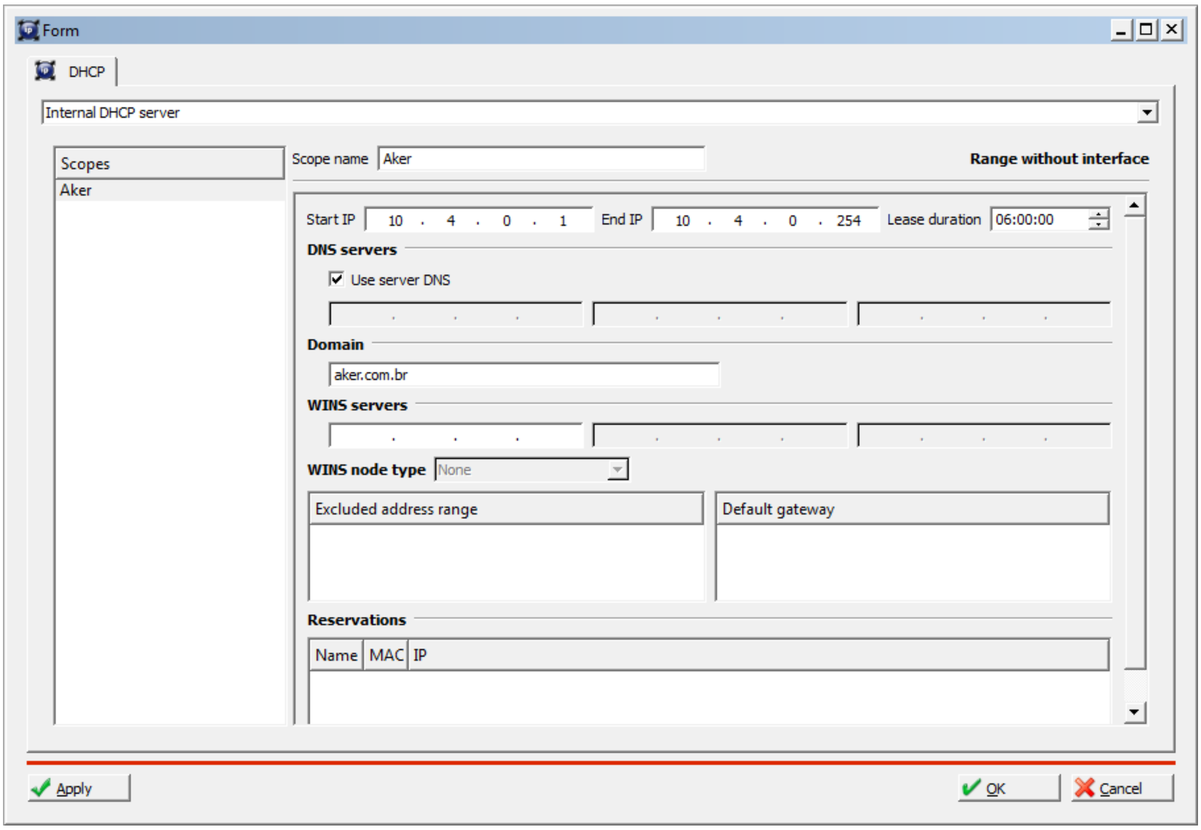

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
DHCP
DNS
Network interfaces
Routing
Tools
Web Content Analyzer

Image 516 – Access window: DHCP.

- Click on the *TCP/IP* menu.
- Select the *DHCP*

The following window will be displayed:



Internal DHCP server

Scopes
Aker

Scope name Aker

Range without interface

Start IP 10 . 4 . 0 . 1 End IP 10 . 4 . 0 . 254 Lease duration 06:00:00

DNS servers

☑ Use server DNS

Domain

aker.com.br

WINS servers

WINS node type None

Excluded address range

Default gateway

Reservations

Name	MAC	IP

Image 517 – DHCP (server)

In this tab the firewall options related to the DHCP server are set. It consists of the following options:

Not using DHCP: Selecting this option, the firewall will not use the DHCP server neither perform the relay among networks connected to it.

DHCP relay between networks: Allows the firewall to perform the DHCP packet relay among the selected networks. This option is used when there is only one DHCP server and you wish to provide addressed to hosts located in distinct subnetwork, directly connected to the firewall.

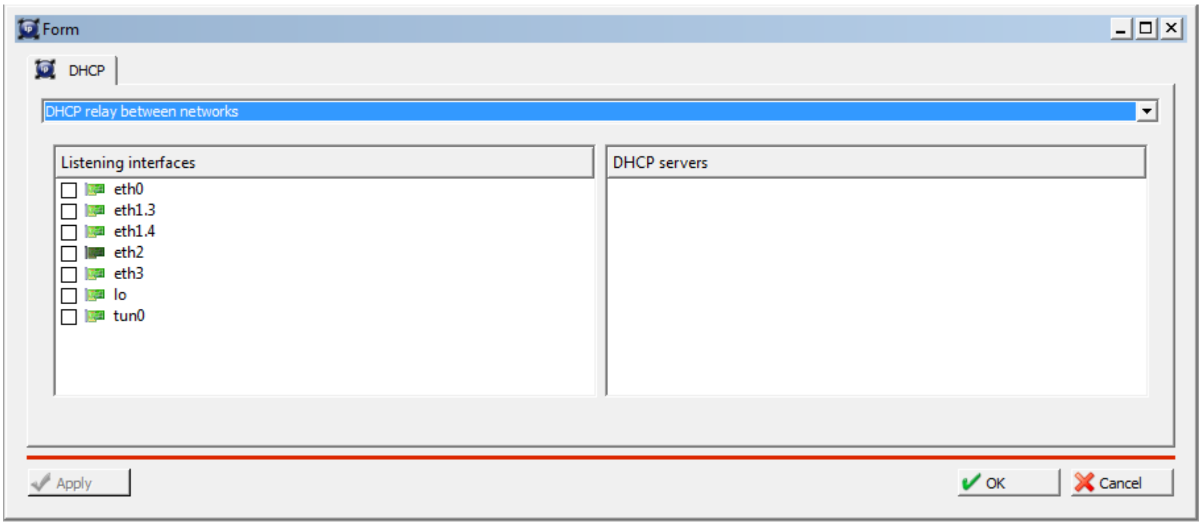
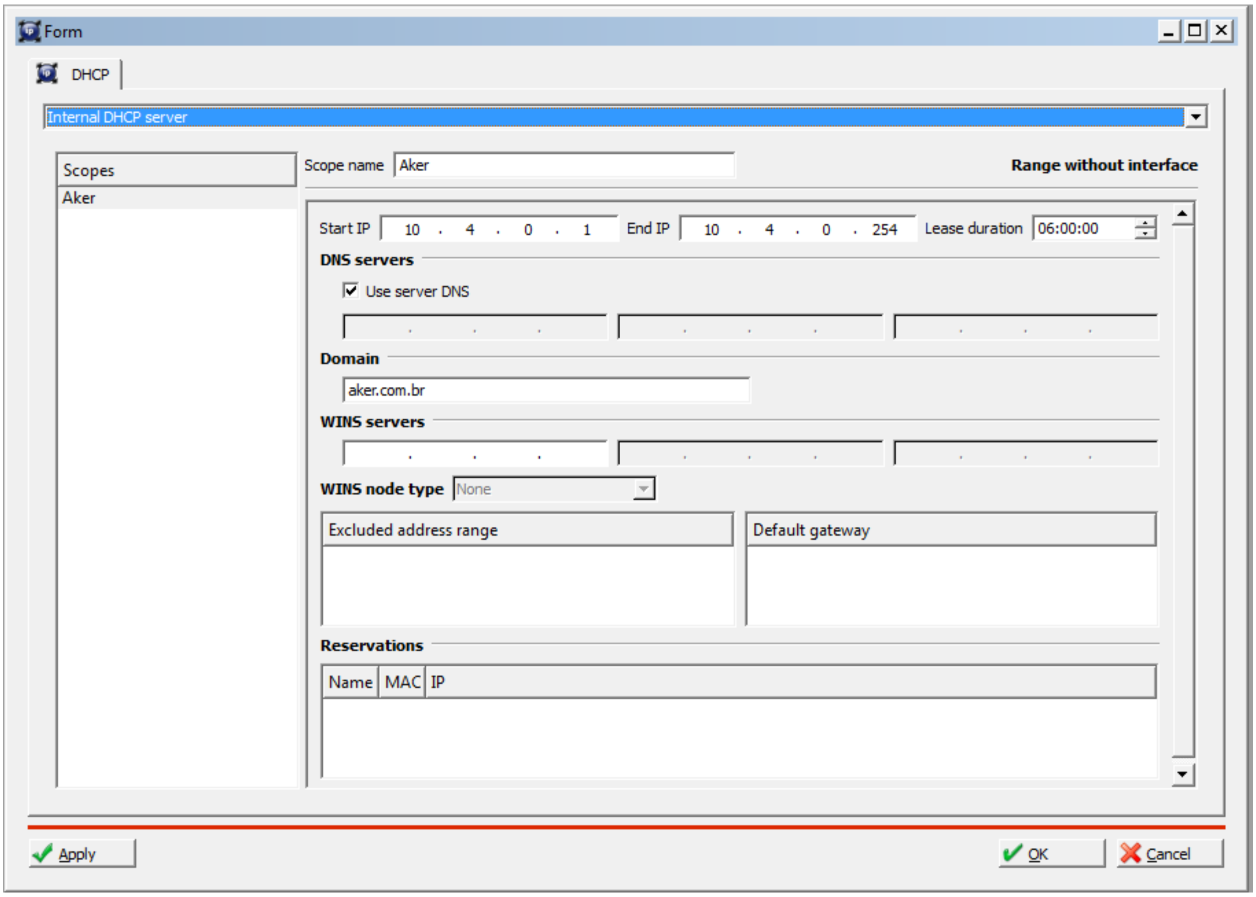

Form
DHCP
DHCP relay between networks
Listening interfaces
☐ eth0
☐ eth1.3
☐ eth1.4
☐ eth2
☐ eth3
☐ lo
☐ tun0
DHCP servers
Apply
OK
Cancel

Image 518 – DHCP relay among en.

Selecting this option, it is required to specify in the **Listening Interfaces** the interfaces which the firewall will listen DHCP broadcasts and will forward them to the servers specified in **DHCP Server.**

Internal DHCP server: This option is designated to small networks that do not have a DHCP server or have it in an ADSL modem. It allows the firewall acts as a DHCP server.


Form
DHCP
Scopes
Excluded address range
Default gateway
Reservations
Name
MAC
IP
Apply
OK
Cancel

Internal DHCP server

Scopes: Aker

Scope name: Aker

Range without interface

Start IP: 10 . 4 . 0 . 1

End IP: 10 . 4 . 0 . 254

Lease duration: 06:00:00

DNS servers

☑ Use server DNS

Domain

aker.com.br

WINS servers

WINS node type: None

Image 519 – Internal DHCP server.

Selecting this option, it is required to specify one or more *Address Scopes, i.e. the* address range, DNS configuration, Wins/NBT and WINS/NBT Node Type, exception, default gateway, and IP address reservations that will be assigned to clients.

The firewall will send to clients its addresses such as the DNS server and its domain, as domain name to these clients.

36.3. DNS

To access the DNS window follow the steps below:

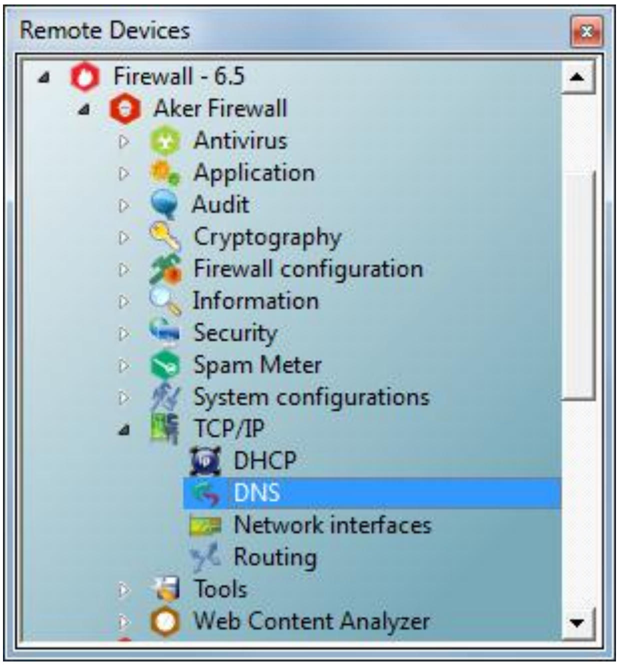
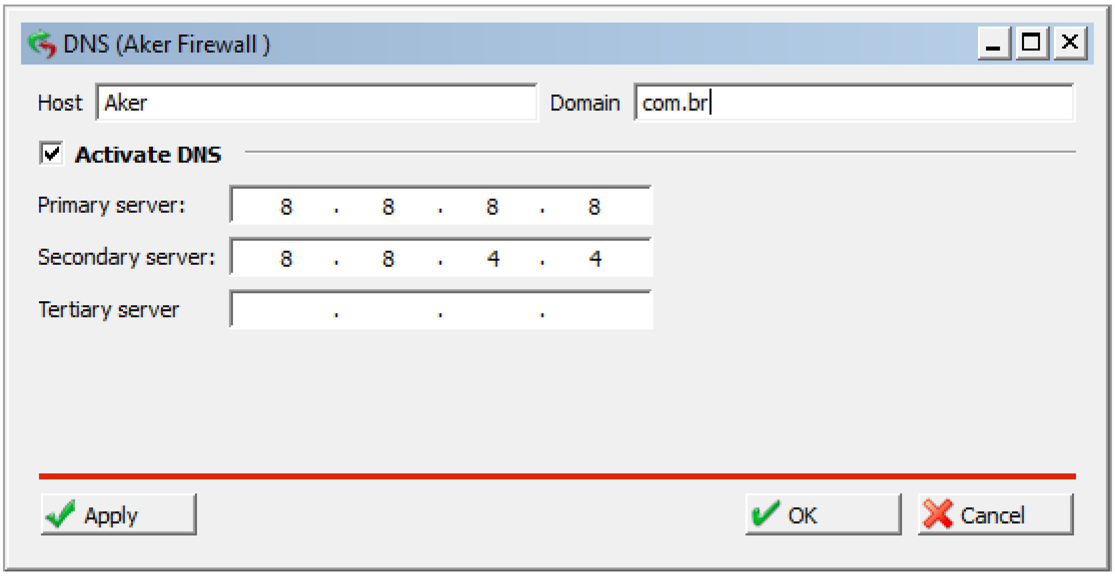

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
DHCP
DNS
Network interfaces
Routing
Tools
Web Content Analyzer

Image 520 – Access window: DNS.

- Click on the *TCP/IP menu.*
- Select *DNS.*

The Image below will be displayed:



DNS (Aker Firewall)

Host: Aker

Domain: com.br

☑ Activate DNS

Primary server: 8 . 8 . 8 . 8

Secondary server: 8 . 8 . 4 . 4

Tertiary server: . . .

Image 521 – TCP/IP – DNS

All options related to name or DNS resolution are configured in the DNS tab. It has the following fields:

Host: Name of the host which the firewall is running.

Domain: Name of domain in which the firewall is running.

Activate DNS: This option must be checked to activate name resolution via DNS, or unchecked to deactivate it.

Primary server: This field defines the primary DNS server. It is mandatory if the *Activate DNS* option is checked.

Secondary server: This field defines the secondary DNS server that will be consulted if the primary fails. It is optional.

Tertiary server: This field defines the tertiary DNS server that will be consulted if the primary and secondary fail. It is optional.

36.3.1. Network interfaces

To gain access to the Network interfaces configuration window, follow the steps below:

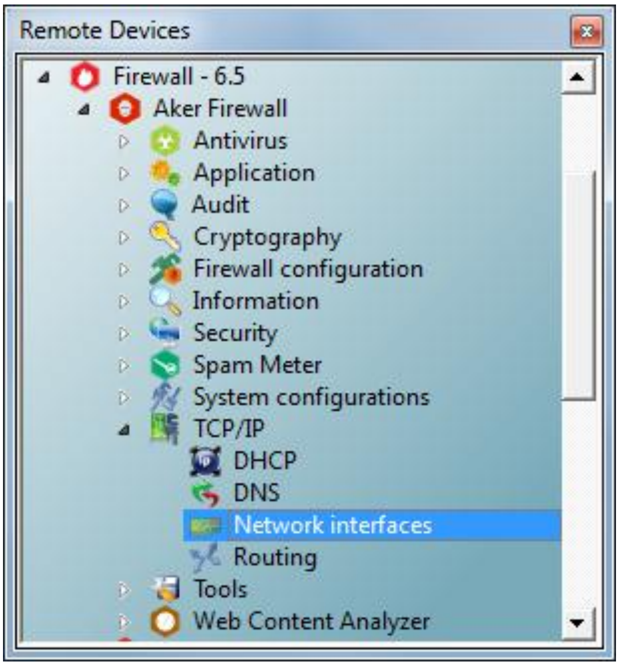
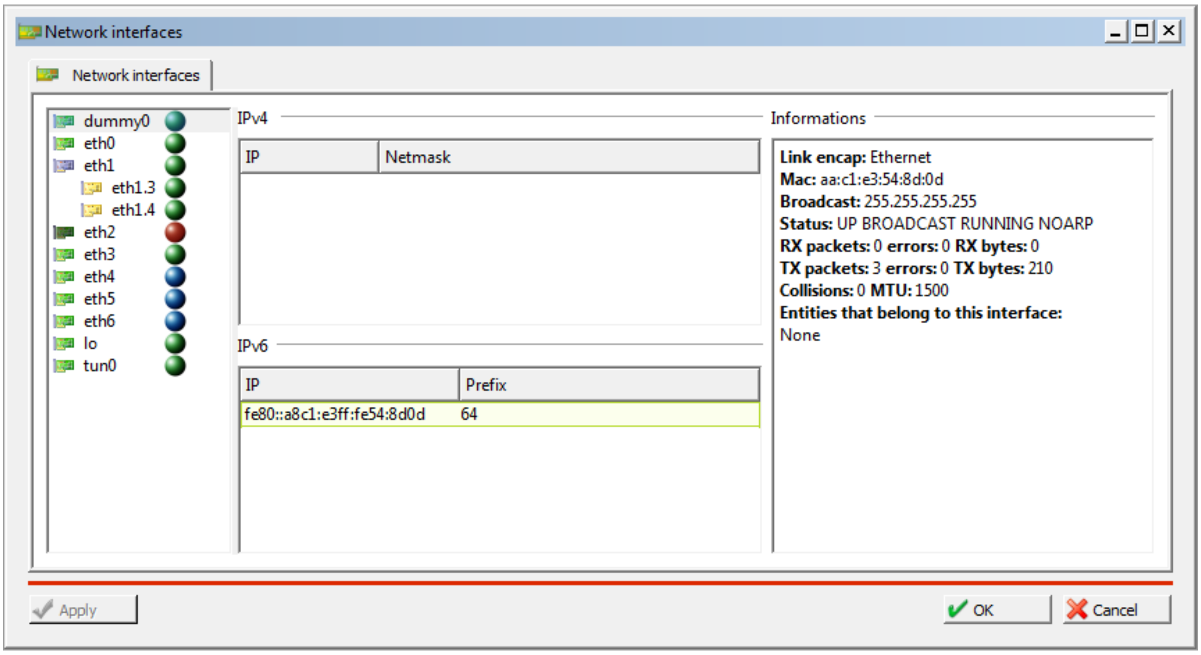

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
DHCP
DNS
Network interfaces
Routing
Tools
Web Content Analyzer

Image 522 – Access window: Network interfaces.

The Image below will be displayed:


Network interfaces
Network interfaces
dummy0
eth0
eth1
eth1.3
eth1.4
eth2
eth3
eth4
eth5
eth6
lo
tun0
IPv4
IP
Netmask
IPv6
Informations
Apply
OK
Cancel

IP	Prefix
fe80::a8c1:e3ff:fe54:8d0d	64

Link encap: Ethernet
Mac: aa:c1:e3:54:8d:0d
Broadcast: 255.255.255.255
Status: UP BROADCAST RUNNING NOARP
RX packets: 0 **errors:** 0 **RX bytes:** 0
TX packets: 3 **errors:** 0 **TX bytes:** 210
Collisions: 0 **MTU:** 1500
Entities that belong to this interface:
None

Image 523 – Access window: Network interfaces.

In this tab the IP addresses assigned to all network interfaces recognized by the firewall. It consists of a list where the names of all interfaces, IP addresses, and mask of each one of them (it is possible to configure up to 31 distinct addresses for each interface)

IPv4

IP: Network address. A self-configured address cannot be informed.

Netmask: Informs the network mask address.

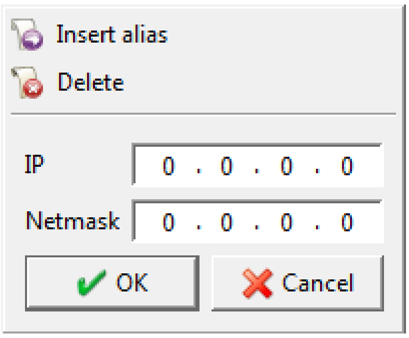
IPv6

IP: Network address. A self-configured address cannot be informed.

Prefix: Informs the amount of bits that compose the network.

Alias

To configure or change the IP address or a mask of an interface, and even assign an *alias* to the interface, click on the device entry and use the following menu:


Insert alias
Delete
OK
Cancel

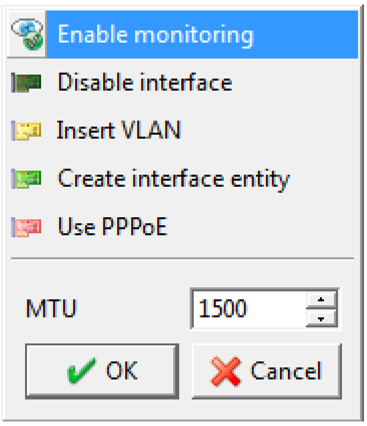
IP 0 . 0 . 0 . 0

Netmask 0 . 0 . 0 . 0

Image 524 – IP address configuration menu.

VLAN

To create a VLAN associated to an interface, click on the desired interface and the following menu will be displayed:


Enable monitoring
Disable interface
Insert VLAN
Create interface entity
Use PPPoE
OK
Cancel

MTU 1500

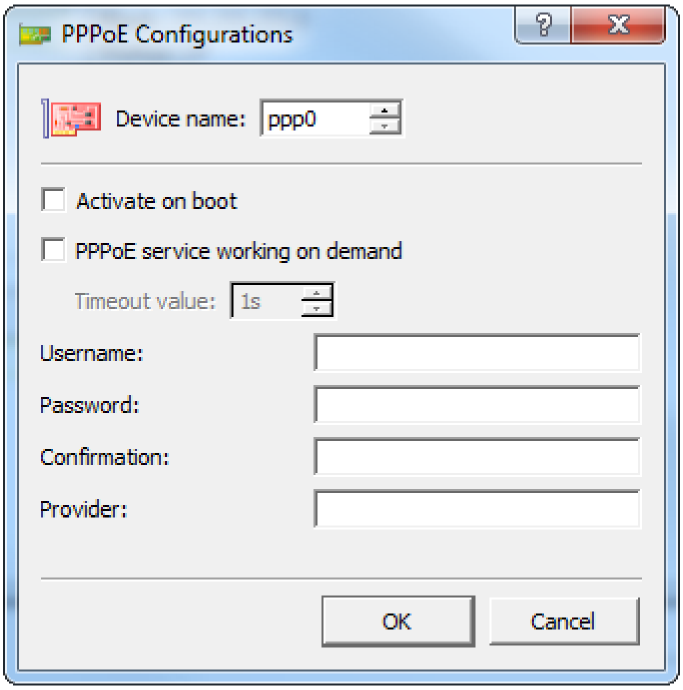
Image 525 –VLAN menu.

A VLAN uses the VLAN tagging (802.1q) system to allow that with a single connection the switch has access to all of its VLANs, and also controlling the access among them. For each one of them a virtual interface will be created inside the firewall.

In this menu it is also possible to ***enable monitoring***, allowing the monitoring of all cluster network interfaces and session details, identifying possible failures, in case a cluster node interface fail (connectivity failure or route failure, or etc.). The cluster node will deactivate all other interfaces and make the other node take control, allowing a greater availability of links.

PPPoE

The **PPPoE** option allows defining that this specific interface works together with the PPPoE (used basically for connections with ADSL modems). When selecting this option the following window will be displayed:



PPPoE Configurations

Device name: ppp0

☐ Activate on boot

☐ PPPoE service working on demand

Timeout value: 1s

Username:

Password:

Confirmation:

Provider:

Image 526 – PPPoE configuration.

Device name: This field indicates the internal device name that will be used in the PPPoE communication. It is important that in case there are more than one interface working in PPPoE, they need to be distinct.

Activate on boot: If this option is selected, the firewall will activate the PPPoE automatically when the machine initiates.

PPPoE service working on demand: If this option is checked, the firewall will activate the PPPoE service only when there be a network traffic redirected through this network interface.

Username: Username that will be used in the authentication during the PPPoE session establishing.

Password: Password that will be used in the authentication during the PPPoE session establishing.

Confirmation: Password confirmation that will be used in the authentication during the PPPoE session establishing.

Provider: The PPPoE server provider.

The IP protocol allows the packet fragmentation, making possible that a datagram be divided into pieces, each of them small enough to be transmited by a connection with the MTU smaller than the original datagram. This fragmentaion is performed in the IP layer (OSI model layer 3) and uses the network interface MTU parameter that will send the through the connection. The MTU path defines the larger MTU value that can pass through the path without risking its packets fragmantation later.

It is only possible to configure network interface IP address recognized by the operating system which the firewall is running. In case a new network interface has been added recently and its name does not appear in the interface list, it is necessary to configure the operation system in order to recognize this new interface before attempting to configure it in this tab. Default value 1500.

IP and prefix have to be informed together.

User will not be possible to remove or edit the self-configured addresses (that are derived from MAC addresses)

Interfaces in red, indicates that they are not present in all cluster nodes.

36.4. Routing

To gain access to the Routing configuration window, follow the steps below:

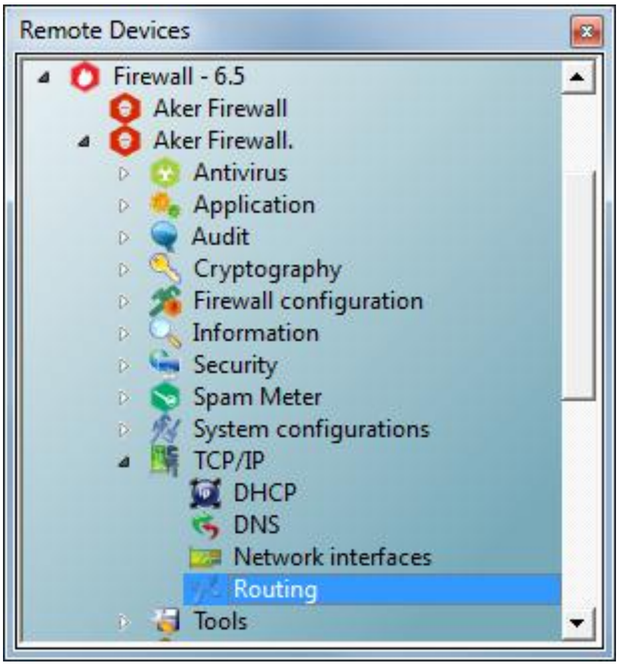
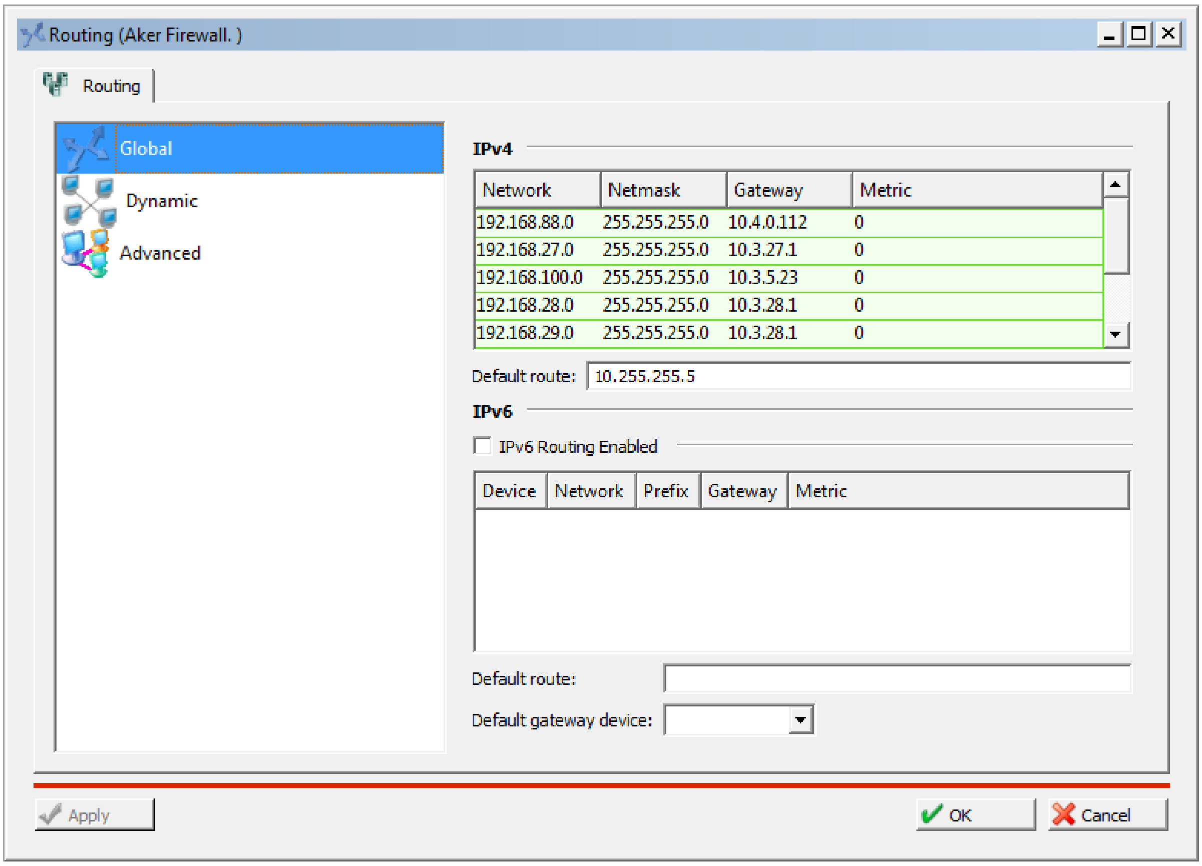

Remote Devices
Firewall - 6.5
Aker Firewall
Aker Firewall.
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
DHCP
DNS
Network interfaces
Routing
Tools

Image 527 – Access window: Routing

- Click on the *TCP/IP* menu.
- Select *Routing.*

The following window will be displayed:


Routing (Aker Firewall.)
Routing
Global
Dynamic
Advanced
IPv4
IPv6
Apply
OK
Cancel

Network	Netmask	Gateway	Metric
192.168.88.0	255.255.255.0	10.4.0.112	0
192.168.27.0	255.255.255.0	10.3.27.1	0
192.168.100.0	255.255.255.0	10.3.5.23	0
192.168.28.0	255.255.255.0	10.3.28.1	0
192.168.29.0	255.255.255.0	10.3.28.1	0

Default route: 10.255.255.5

☐ IPv6 Routing Enabled

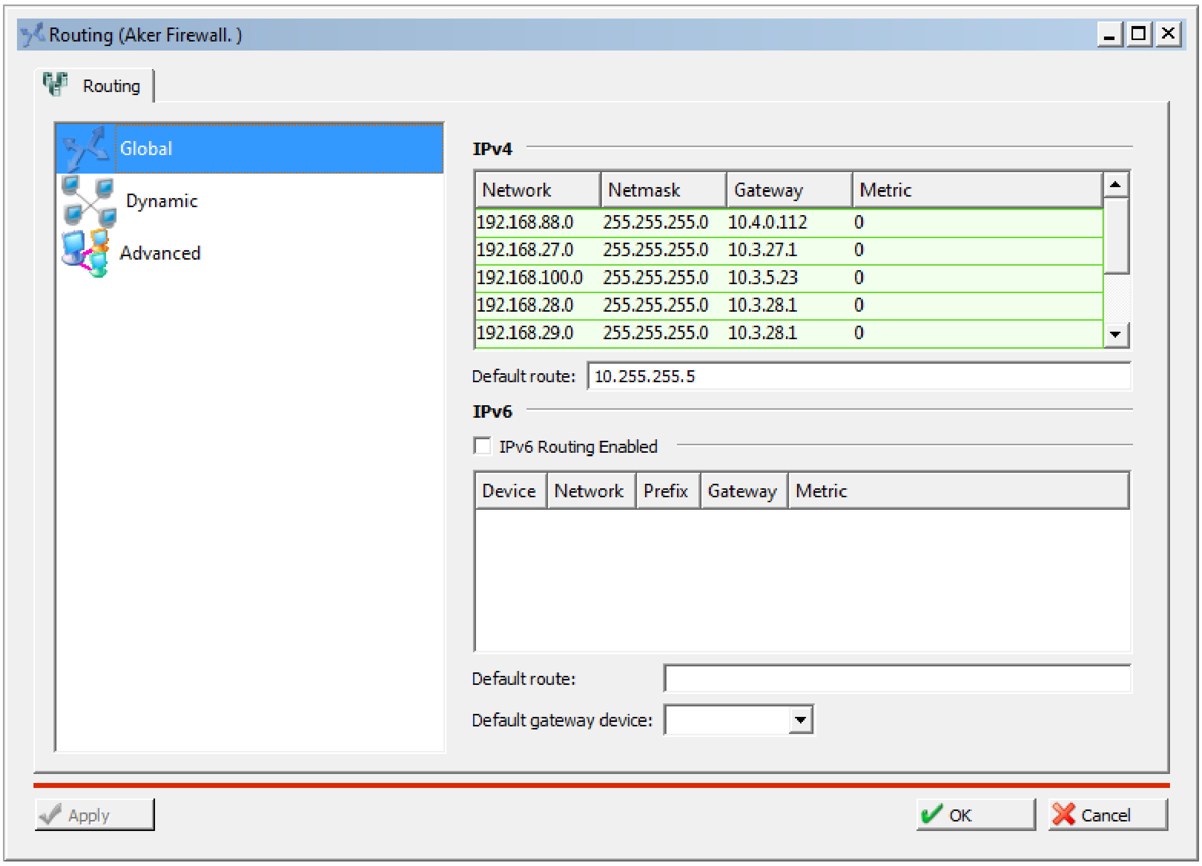
Device	Network	Prefix	Gateway	Metric

Default route:

Default gateway device:

Image 528 – Routing window

36.4.1. Global



Network	Netmask	Gateway	Metric
192.168.88.0	255.255.255.0	10.4.0.112	0
192.168.27.0	255.255.255.0	10.3.27.1	0
192.168.100.0	255.255.255.0	10.3.5.23	0
192.168.28.0	255.255.255.0	10.3.28.1	0
192.168.29.0	255.255.255.0	10.3.28.1	0

Default route: 10.255.255.5

☐ IPv6 Routing Enabled

Device	Network	Prefix	Gateway	Metric

Default route:

Default gateway device:

Image 529 – Routing – Global tab

This window configures the IPv4 and IPv6 in the firewall. It consists of two parts:

The first part configures the IPv4, below follows the description its fields field:

Network: IP address configuration

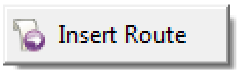
Netmask: Informs the network mask address

Gateway: In this field shall be informed the router IP address.

Metric: Is the network distance value. The distance can be measured by device number that the packet shall pass through, time taken from the source to destination, or a value assigned to the link.

Default route: Specifies the default router, which all packets will be forwarded.

To add a new route simply right-click, and select the "**Insert route**" option.



.

The second part configures the IPv6, below follows the description of its fields:

IPV6 Routing Enabled: This option activates or deactivates the IPv6 packet routing.

Device: Defines the Network Interface used for static route.

Network: IP address configuration

Prefix: Informs how many bits the network is composed of. Values go from 0 to 128.

Gateway: In this field shall be informed the router IP address.

Metric: Is the network distance value. The distance can be measured by: device number that the packet shall pass through, time taken from the source to destination, or a value assigned to the link.

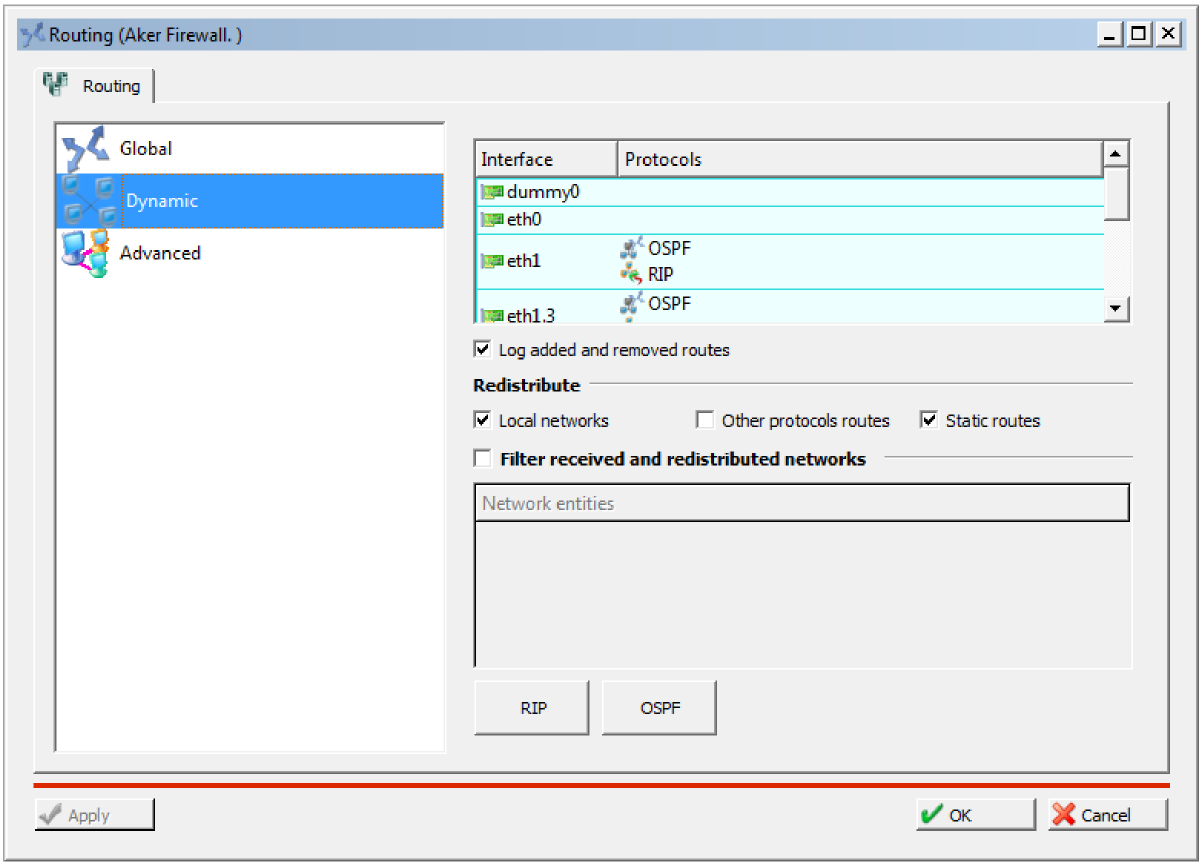
Default Gateway: In this field the default route IP address need to be informed. The IPv6 address validation applies to this field as well.

Default gateway device: Specifies the default router, which all packets will be forwarded. It can be left in blank, but it will not be optional if the default gateway is self-configured.

Routes with link scope are the ones the start with prefix fe80 defined in the macro FWTCPIP_IPV6_AUTOCONF_PREFIX.

Due to a limitation of Linux, it is not possible to remove the IPv6 module once it has been installed, also if the module was not installed on Kernel, all daemons were listening an IPv4 socket. This way modifying this option value, the GUI shall give you the following message: “This setting will be fully functional only after the next firewall reboot”.

36.4.2. Dynamic



Interface	Protocols
dummy0	
eth0	
eth1	OSPF RIP
eth1.3	OSPF

☑ Log added and removed routes

Redistribute

☑ Local networks ☐ Other protocols routes ☑ Static routes

☐ **Filter received and redistributed networks**

Network entities

Image 530 – Routing (dynamics)

Static routing normally is manually configured, the routing table is static, routes do not change dynamically according with the network topology changes, the maintenance cost grows according to the complexity and network size, and configuration failures are expected.

Dynamic routing is the propagation and the changes of routing tables in a dynamic way, it does not have the administrator intervention all the time, the tables are dynamically changed according to the network topology, and i.e. the process is adaptive and improves the maintenance in large networks, and configuration failures are expected as well.

In this window the Dynamic routing configurations are set. It consists of the following options:

Interface: The interlacing used to reach the next router of the destination route.

Protocols: You may choose between RIP protocol or OSPF.

RIP: The **Routing Information Protocol** (**RIP**) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the so called RMTI (**R**outing Information Protocol with **M**etric-based **T**opology **I**nvestigation) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

Originally each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would spread out in time, but this was not true in practice. Sally Floyd and Van Jacobson showed in 1994 that, without slight randomization of the update timer, the timers synchronized over time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS (the latter two being link-state routing protocols), and (without RMTI) a hop limit severely limits the size of network it can be used in. However, it is easy to configure, because RIP does not require any parameters on a router unlike other protocols

- **Advantages**: In small networks it does not consume a lot of bandwidth and configuration and management time, and it is easy to be implemented;

  Disadvantages: Slow convergence for middle and large network. The existence of loops and count-to-infinity, Lops' number limited to 15 per path and metric limitation.

OSPF: **Open Shortest Path First** (**OSPF**) is a link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, very quickly and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The **link-state** information is maintained on each router as a link-state database (LSDB) which is a tree-image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF routers.

The OSPF routing policies to construct a route table are governed by link cost factors (*external metrics*) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unit less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network may be structured, or subdivided, into routing *areas* to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.

By convention, area 0 (zero) or 0.0.0.0 represents the core or *backbone* region of an OSPF network. The identifications of other areas may be chosen at will; often, administrators select the IP address of a main router in an area as the area's identification. Each additional area must have a direct or virtual connection to the backbone OSPF area. Such connections are maintained by an interconnecting router, known as *area border router* (ABR). An ABR maintains separate link state databases for each area it serves and maintains summarized routes for all areas in the network.

OSPF does not use a TCP/IP transport protocol (UDP, TCP), but is encapsulated directly in IP datagrams with protocol number 89. This is in contrast to other routing protocols, such as the Routing Information Protocol (RIP), or the Border Gateway Protocol (BGP). OSPF handles its own error detection and correction functions.

- **Advantages**: Greater convergence speed, support to several metrics, multiple path, no loop or count-to-infinity and synchronism between databases.

  Disadvantages: Complexity in the management and implantation.

  OSPF cost: The OSPF cost also known as metric. The best way has the lowest cost, being typically the one with higher bandwidth. The route cost to reach a specific place.

OSPF speed: The link speed, i.e. the connection speed between two routers which is informed in Kbits/sec.

OSPF area: The area is a designation assigned to a subset of routers and networks that constitute the AS (Autonomous System).

Log added and removed routes: Selecting this option, added and removed routes will be displayed in the events list.

Redistribute: In this option, you select the routes that will be redistributed to the routers.

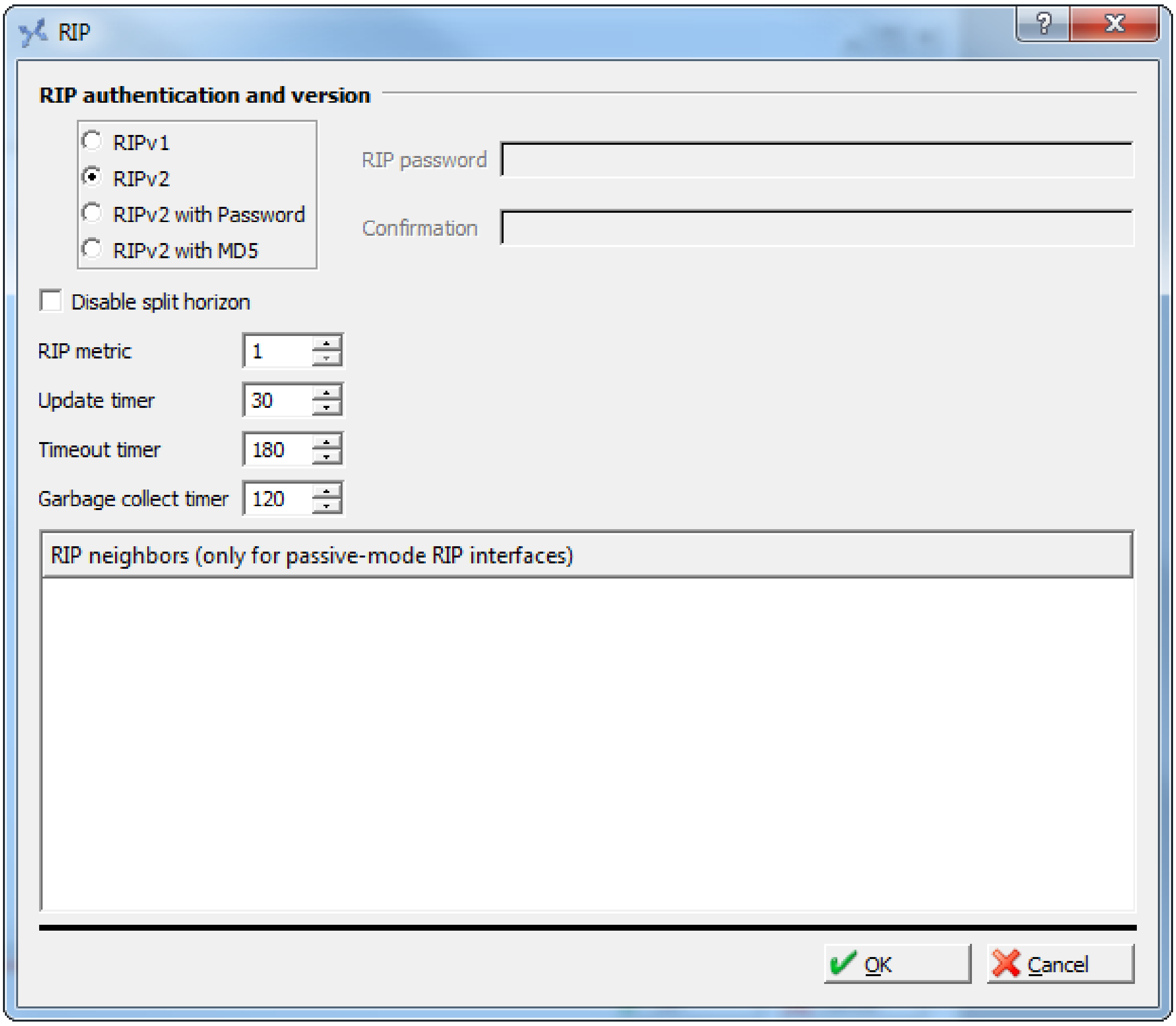
Local networks: They are routes locally connected that match to the subnetwork configured in the network interfaces.

Other protocols routes: Selecting this option, the redistributed routes will be specified by the RIP and OSPF protocol. There will be an exchange of information in the communication between them, i.e. what has been learned by a protocol shall be informed by the other protocol and vice versa.

Static routes: Fixed routes which the data will be transmitted. Static routes are configured by the administrator.

Filter received and redistributed networks: Selecting this option, you need to specify the networks and hosts you wish to receive and distribute new routes through the RIP and OSPF protocol.

RIP



RIP authentication and version

○ RIPv1
● RIPv2
○ RIPv2 with Password
○ RIPv2 with MD5

RIP password

Confirmation

☐ Disable split horizon

RIP metric: 1

Update timer: 30

Timeout timer: 180

Garbage collect timer: 120

RIP neighbors (only for passive-mode RIP interfaces)

Image 531 – Routing- Dynamic (RIP)

RIP authentication and version

This option allows you to choose the protocol authentication type. It is strongly recommended that you choose the RIPv2 with MD5, because it is the safest way to authenticate.

RIPv1: No authentication. Only the data will be sent.

RIPv2: No authentication. Only the data will be sent.

RIPv2 with Password: Contains authentication. The data and secret will be sent.

RIPv2 with MD5: Authentication with MD5. The data will be sent together with the digital signature which contains the secret.

RIP password: The protocol authentication password.

Confirmation: Retype the protocol authentication password in order to confirm the RIP password.

RIP neighbors options: This option sets the routers and protocols that will establish the communication. This field is required only when the passive mode operation is being used.

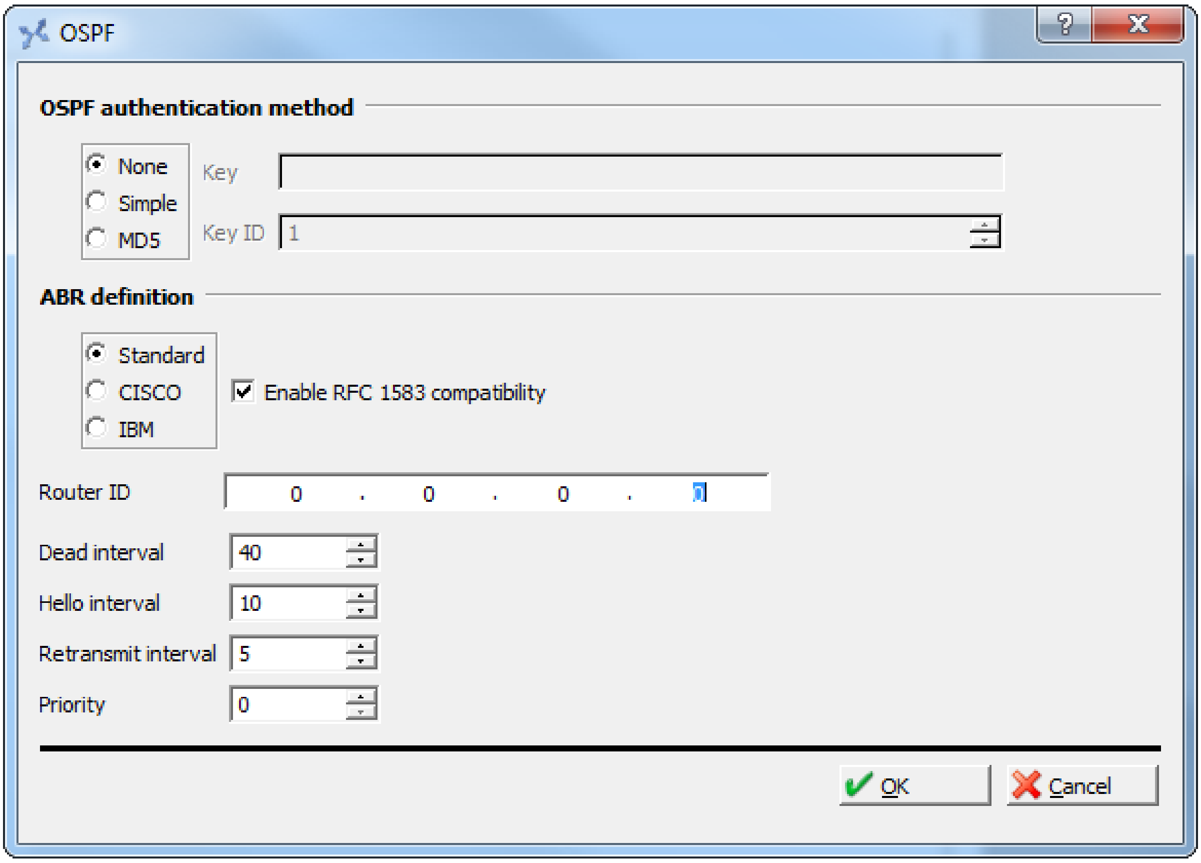
RIP metric: It is the network distance value. This distance can be measured by a number of devices that the packet must to pass through. Normally the metric is incremented by RIPD when the information is received. The metric of distributed routes is set as 1.

Update timer: The default update time is 30 seconds. Each time it expired RIP process sends an unsolicited message containing routing table to all neighboring RIP routers.

Timeout timer: After the Timeout expires, the router is taken as out of operation; however for a brief period the information about this router is kept in the routing table, in order to notify the neighbors that is has been removed. Default timeout is 180 seconds.

Garbage collect timer: Time that the firewall takes to consider a route as expired.

OSPF



OSPF

OSPF authentication method

● None
○ Simple
○ MD5

Key:

Key ID: 1

ABR definition

● Standard
○ CISCO
○ IBM

☑ Enable RFC 1583 compatibility

Router ID: 0 . 0 . 0 . 0

Dead interval: 40

Hello interval: 10

Retransmit interval: 5

Priority: 0

Image 532 – Routing- Dynamic (OSPF)

OSPF authentication method

This option allows you to choose the most secure form of authentication in the exchange of information between routers, preventing attacks to these routers. It is strongly recommended that you choose the MD5, because it is the safest way to authenticate. The protocol will send all traffic safely after the authentication

None: Does not have authentication.

Simple: Unencrypted key

MD5: Data and key’s hash.

Key: Secret used in the OSPF authentication.

Key ID: Identify which key is being used.

ABR definition

The options below set how the OSPF protocol will distribute the routes between the routers.

- Standard
- CISCO
- IBM

Enable RFC 1583 compatibility: Selecting this option you will use an older standard.

RFC2328 is the successor of RFC1583, it is recommended to change the algorithm path in order to prevent routing loops that can happen when the OSPFv2 is being used.

Router ID: ID address that identifies the router in the OSPF process.

Dead interval: Maximum period in seconds since the last hello packet has been received, before the router considers its “neighbor” as not accessible. The default value is 40 seconds.

Hello interval: Interval in seconds between the hello packet transmissions. Setting this value the hello packets will be sent periodically according to the time specified on the interface. This value must to the same to all routers existing in the network. Default value is 10 seconds.

Retransmit interval: This value is used when the database description and the link state request packet are retransmitted. The default value is 5 seconds.

Priority: Setting a higher priority value, the router will have more chances to become a designated router. Setting the value 0 router will not be the preferable route. Default value is 1.

36.4.3. Advanced

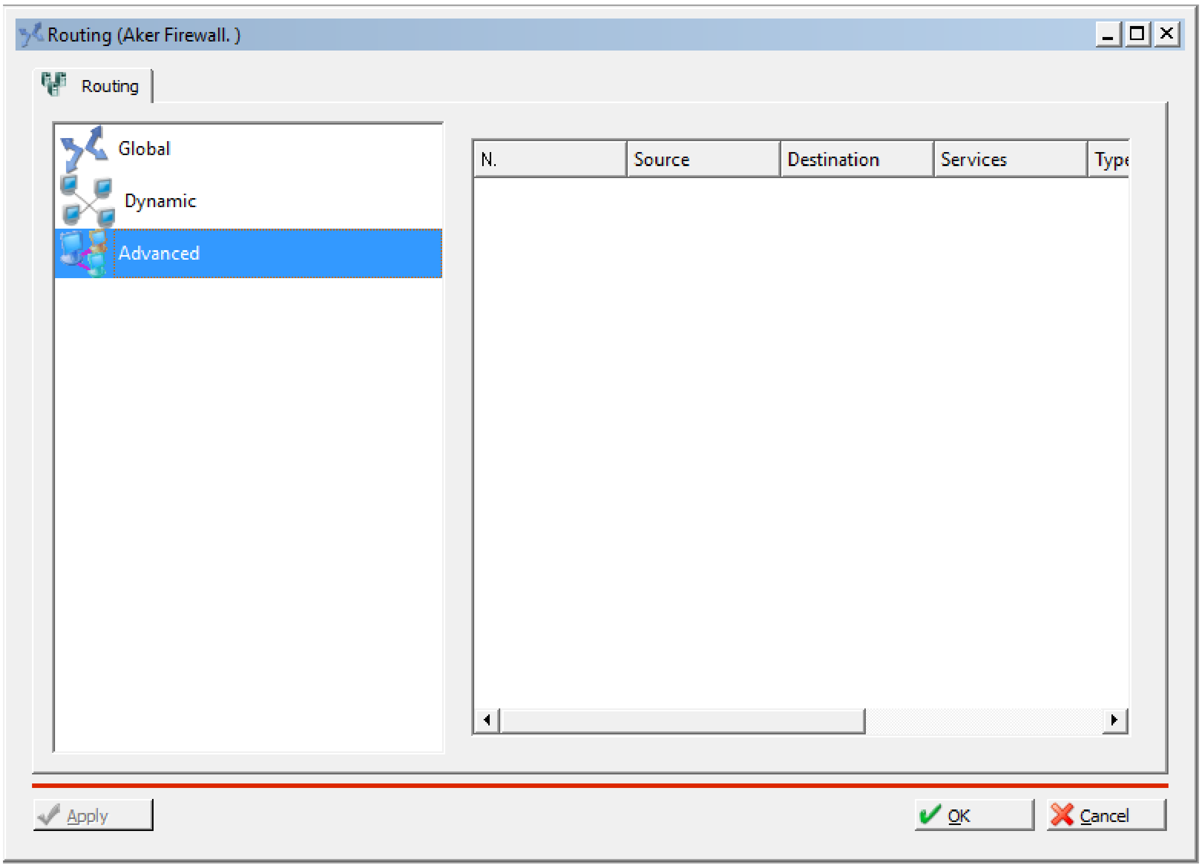

Routing (Aker Firewall.)
Routing
Global
Dynamic
Advanced
N.
Source
Destination
Services
Type
Apply
OK
Cancel

Image 533 – Routing – Advanced.

This configuration allows you use the source routes and link balancing routes, where it is possible to direct the network traffic to a specific gateway from its origin and even balance this traffic in up to 3 distinct links. It is not possible to create source routes in the Global tab, due to it, rules created in the advanced tab have higher priority.

To perform this configuration successfully, it is necessary to register the source, destination and service entities before you start the configuration. You can register it using the Remote Interface of Aker Control Center or use the Text Interface using the “fwent” command.

Below follows some examples of configuration:

Routes load balancing test:

Lab

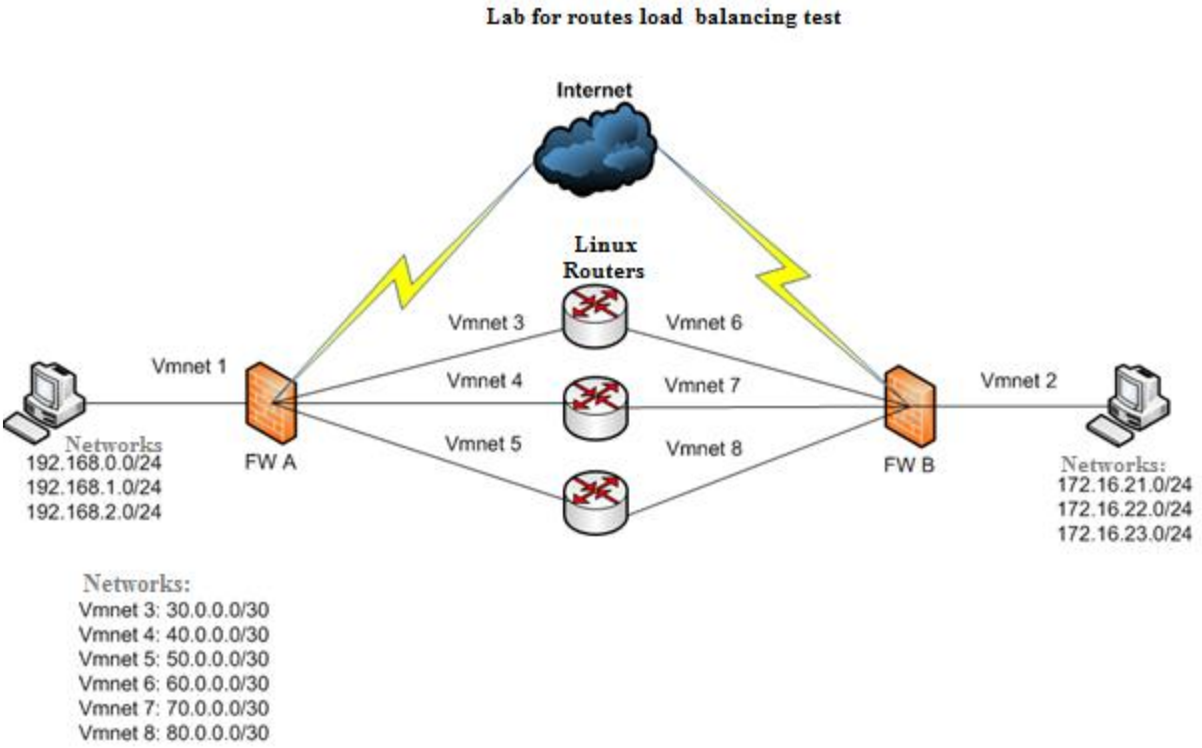
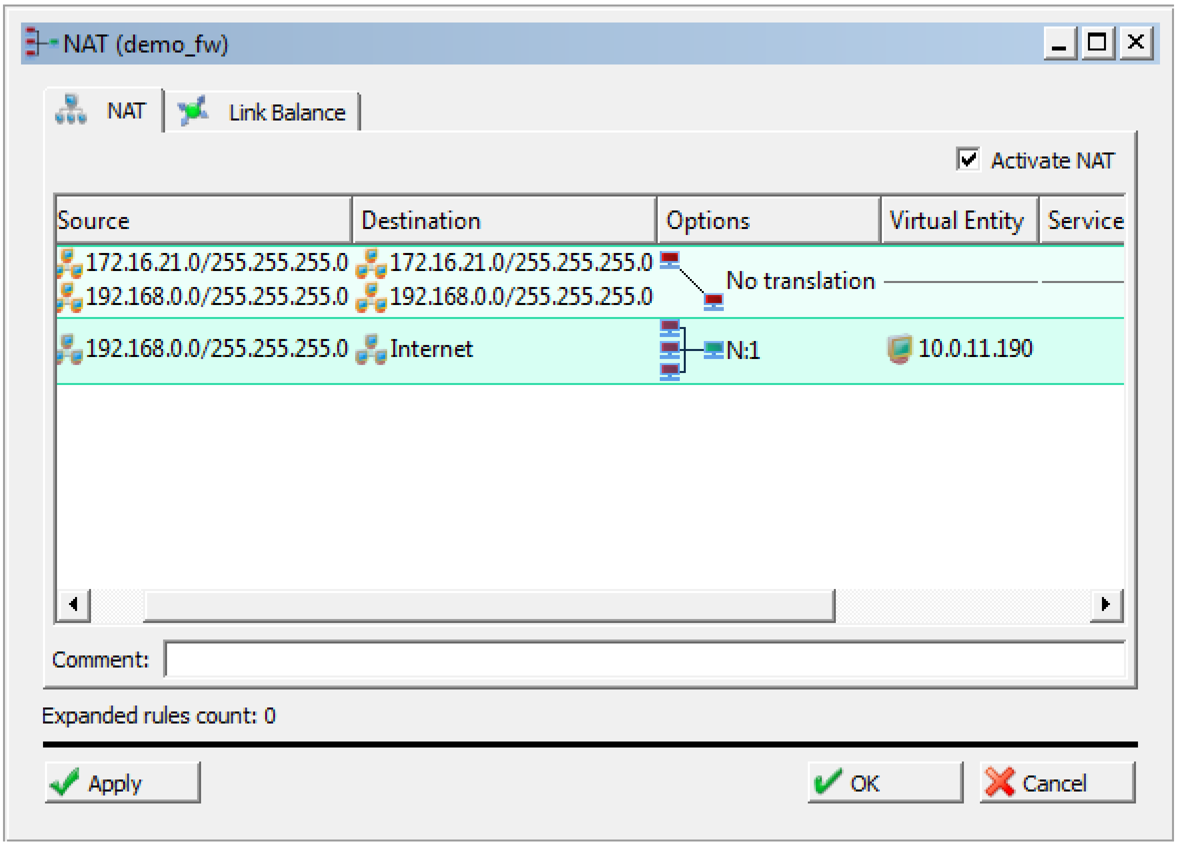

Lab for routes load balancing test
Internet
Linux Routers
Vmnet 1
Vmnet 2
Vmnet 3
Vmnet 4
Vmnet 5
Vmnet 6
Vmnet 7
Vmnet 8
FW A
FW B
Networks
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
Networks:
172.16.21.0/24
172.16.22.0/24
172.16.23.0/24
Networks:
Vmnet 3: 30.0.0.0/30
Vmnet 4: 40.0.0.0/30
Vmnet 5: 50.0.0.0/30
Vmnet 6: 60.0.0.0/30
Vmnet 7: 70.0.0.0/30
Vmnet 8: 80.0.0.0/30

Image 534 – routes balancing.

Configuration Examples

Configuration using the Remote Interface – Nat 1st example:



☑ Activate NAT

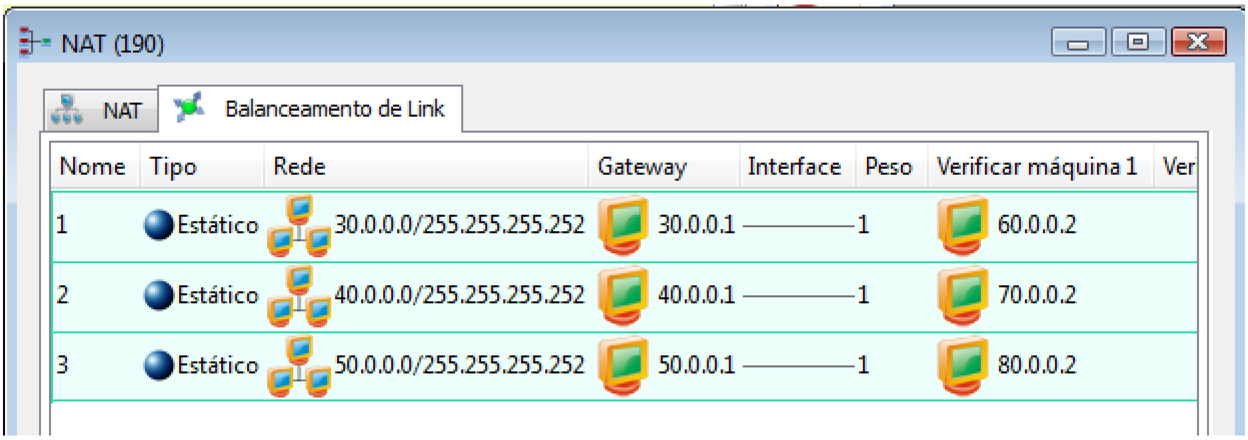
Source	Destination	Options	Virtual Entity	Service
172.16.21.0/255.255.255.0 192.168.0.0/255.255.255.0	172.16.21.0/255.255.255.0 192.168.0.0/255.255.255.0	No translation		
192.168.0.0/255.255.255.0	Internet	N:1	10.0.11.190	

Comment:

Expanded rules count: 0

Image 535 – NAT – 1st example

Configuration using the Remote Interface – Link balance 1st example



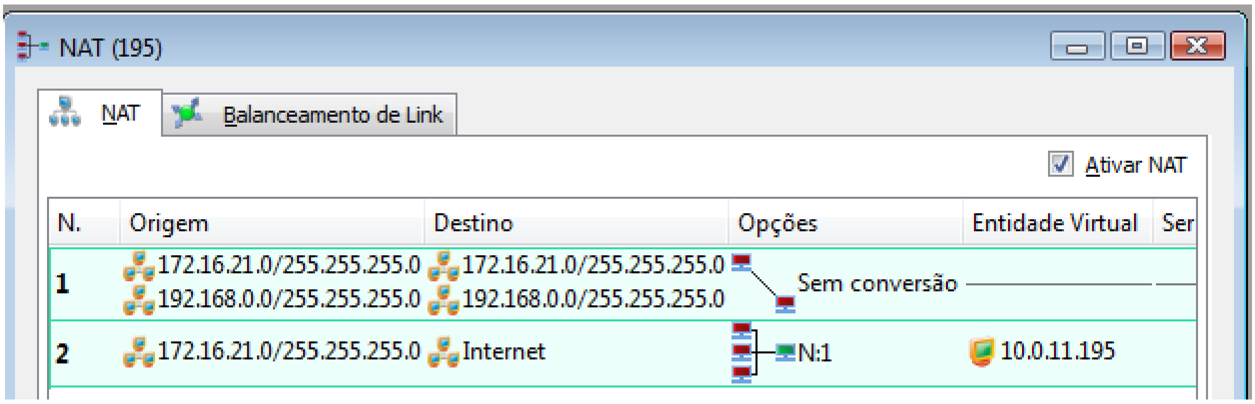
Nome	Tipo	Rede	Gateway	Interface	Peso	Verificar máquina 1	Ver
1	Estático	30.0.0.0/255.255.255.252	30.0.0.1		1	60.0.0.2	
2	Estático	40.0.0.0/255.255.255.252	40.0.0.1		1	70.0.0.2	
3	Estático	50.0.0.0/255.255.255.252	50.0.0.1		1	80.0.0.2	

Image 536 – Link balance **1**st example

Using the Text Interface:

```
fwadvroute add 1 -src 192.168.0.0/255.255.255.0 -dst 172.16.21.0/255.255.255.0 -
bal 1 2 3
```

Configuration using the Remote Interface – Nat 2nd example:

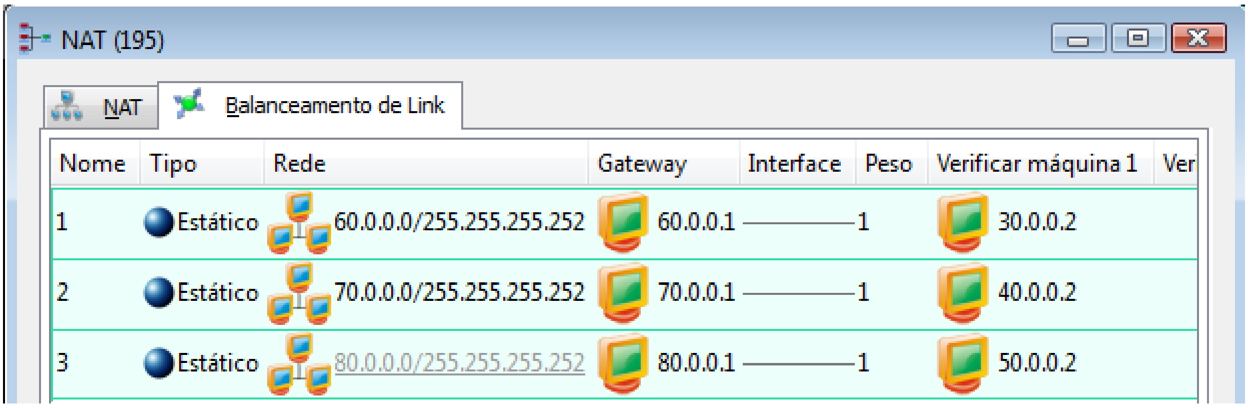


☑ Ativar NAT

N.	Origem	Destino	Opções	Entidade Virtual	Ser
1	172.16.21.0/255.255.255.0 192.168.0.0/255.255.255.0	172.16.21.0/255.255.255.0 192.168.0.0/255.255.255.0	Sem conversão		
2	172.16.21.0/255.255.255.0	Internet	N:1	10.0.11.195	

Image 537 – Nat -2nd example

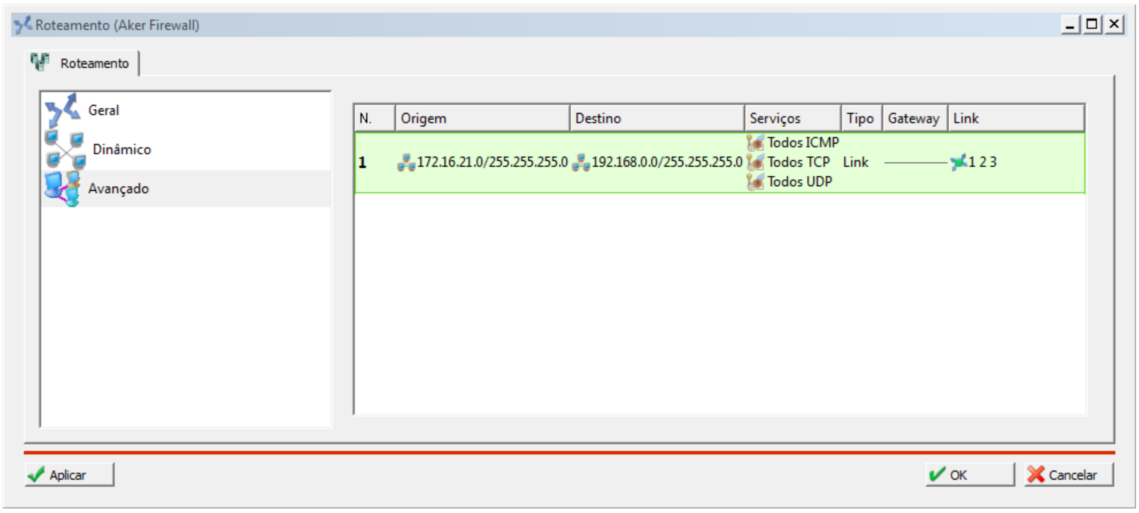
Configuration using the Remote Interface – Link balance 2nd example:



Nome	Tipo	Rede	Gateway	Interface	Peso	Verificar máquina 1	Ver
1	Estático	60.0.0.0/255.255.255.252	60.0.0.1		1	30.0.0.2	
2	Estático	70.0.0.0/255.255.255.252	70.0.0.1		1	40.0.0.2	
3	Estático	80.0.0.0/255.255.255.252	80.0.0.1		1	50.0.0.2	

Image 538 – Link balance – 2nd example

Configuration using the Remote Interface – Routing 2nd example:


Roteamento (Aker Firewall)
Roteamento
Geral
Dinâmico
Avançado
Aplicar
OK
Cancelar

N.	Origem	Destino	Serviços	Tipo	Gateway	Link
1	172.16.21.0/255.255.255.0	192.168.0.0/255.255.255.0	Todos ICMP Todos TCP Todos UDP	Link	———	1 2 3

Image 539 – routing 2nd example

Using the Text Interface:

```
fwadvroute add 1 -src 172.16.21.0/255.255.255.0 -dst 192.168.0.0/255.255.255.0 -bal 1 2 3
```

This configuration causes all traffic between the networks 192.168.0.0/24 and 172.16.21.0/24 be balanced by 3 links.

Using the text interface:

Program location: */aker/bin/firewall # fwadvroute help*

Aker Firewall *-*

```
Usage: fwadvroute help

   fwadvroute show

   fwadvroute add <pos> -src <src_ents> -dst <dst_ents> [-svc <svc_ents>]

 { -gw <gw_ent> | [-P] -bal <link1> <link2> ... }

   fwadvroute delete <pos>

   fwadvroute < enable | disable > <pos>

   fwadvroute refresh
```

The parameters are:

pos: rule's position in the table (from 1);

src_ents : Source entities (network/host/set);

dst_ents : Destination entities (network/host/set);

svc_ents : Service entities (service);

gw_ent : Gateway entities (hosts);

linkN : Names of links for balancing (see 'fwblink show);

-P : Connection persistence.

Below follows some examples of syntaxes used in this configuration.

Syntax: fwadvroute add <pos> -src <src_ents> -dst <dst_ents> [-svc <svc_ents>] -gw <gw_ent>

The syntax above shows how to create or set route specifying its position (pos), source (src), service (svc) (in case there is one), destination(dst) and the chosen gateway (gw). ENT goes for entity.

Example: *fwadvroute add 1 -src "Intranet" -dst host1 -gw server1*

Quotation marks are required when indicating an entity which has more than one word in its name, as the example above “Intranet”.

Syntax: fwadvroute delete <pos>

Deletes an existing rule indicating its position.

Example: *fwadvroute delete 1*

Syntax: fwadvroute < enable | disable > <pos>

Enable or disable a route indicating its position.

Example: *fwadvroute enable 1*

It is not possible to configure source routes through the Control Center, this configuration is done only through the Text Interface.

36.5. Using the Text Interface for Activation Keys

It is possible to configure Activation Keys through the Text Interface.

Program location: /aker/bin/firewall/fwkey path

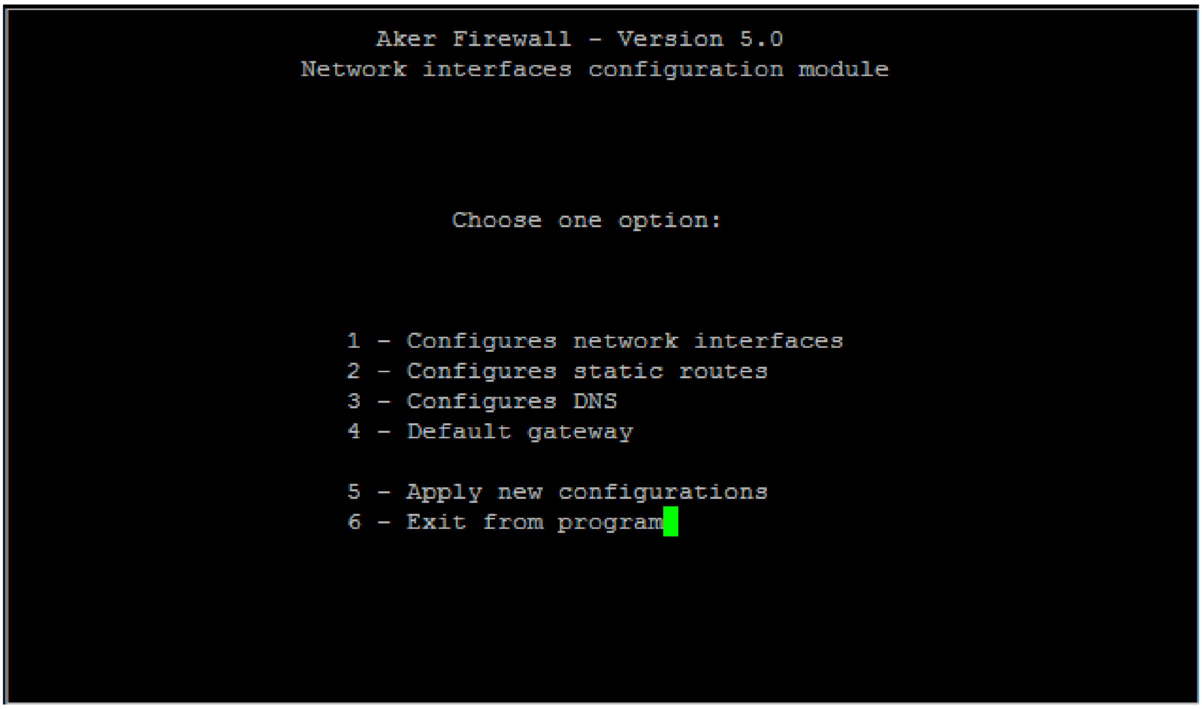
Path: Complete path to files with activation key selected to be replaced.

36.6. Using the Text Interface for TCP/IP configuration

It is possible to configure TCP/IP parameters through the Text Interface.

Program location: /etc/firewall/fwinterface

The program is interactive and the configuration options are described below:

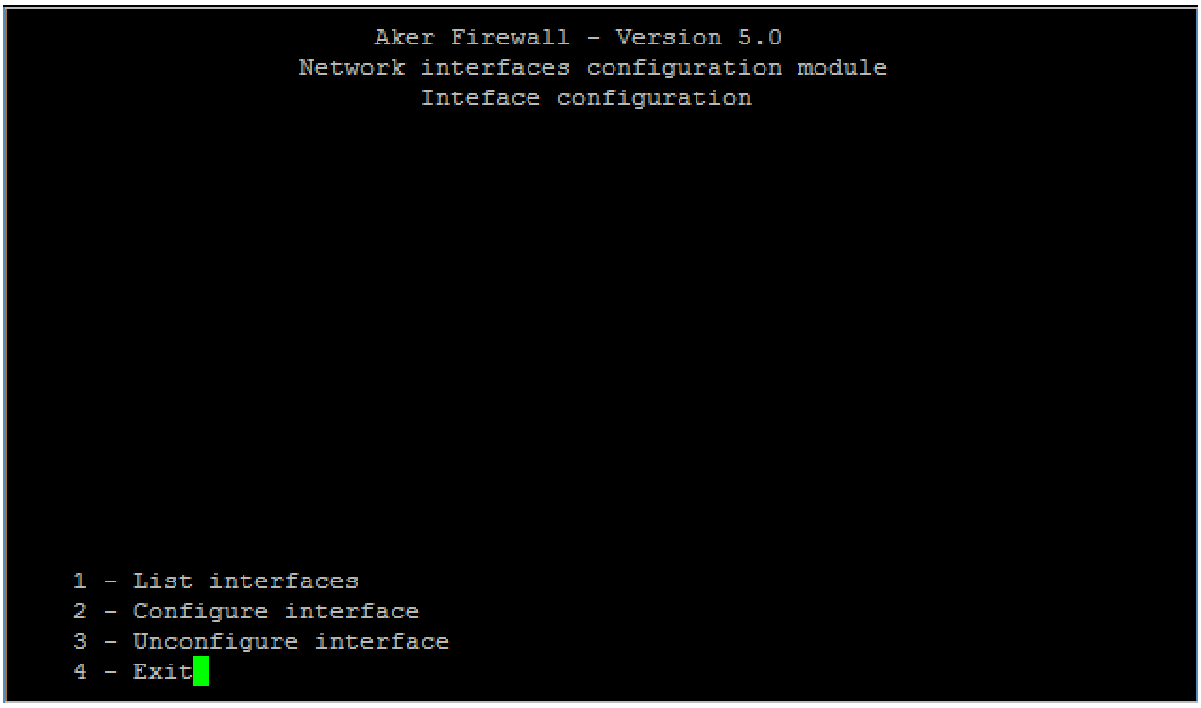


```
                   Aker Firewall - Version 5.0
             Network interfaces configuration module



                      Choose one option:



               1 - Configures network interfaces
               2 - Configures static routes
               3 - Configures DNS
               4 - Default gateway

               5 - Apply new configurations
               6 - Exit from program
```

Image 540 – Network Interfaces configuration module.

Similarly to the GUI, the Text Interface has 6 options, as seen above.

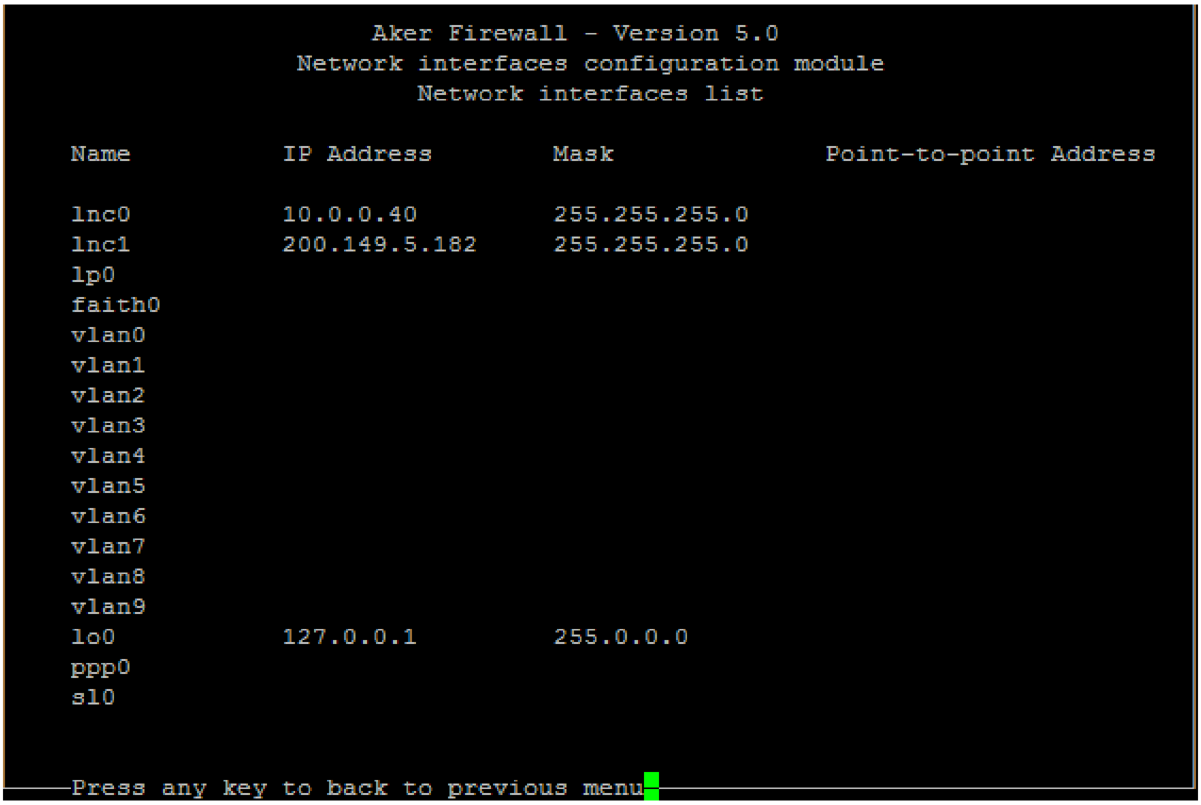
In the window below, it is possible to view, configure and change configuration of a network interface.



```
                    Aker Firewall - Version 5.0
               Network interfaces configuration module
                       Inteface configuration









   1 - List interfaces
   2 - Configure interface
   3 - Unconfigure interface
   4 - Exit
```

Image 541 – Interface configuration.

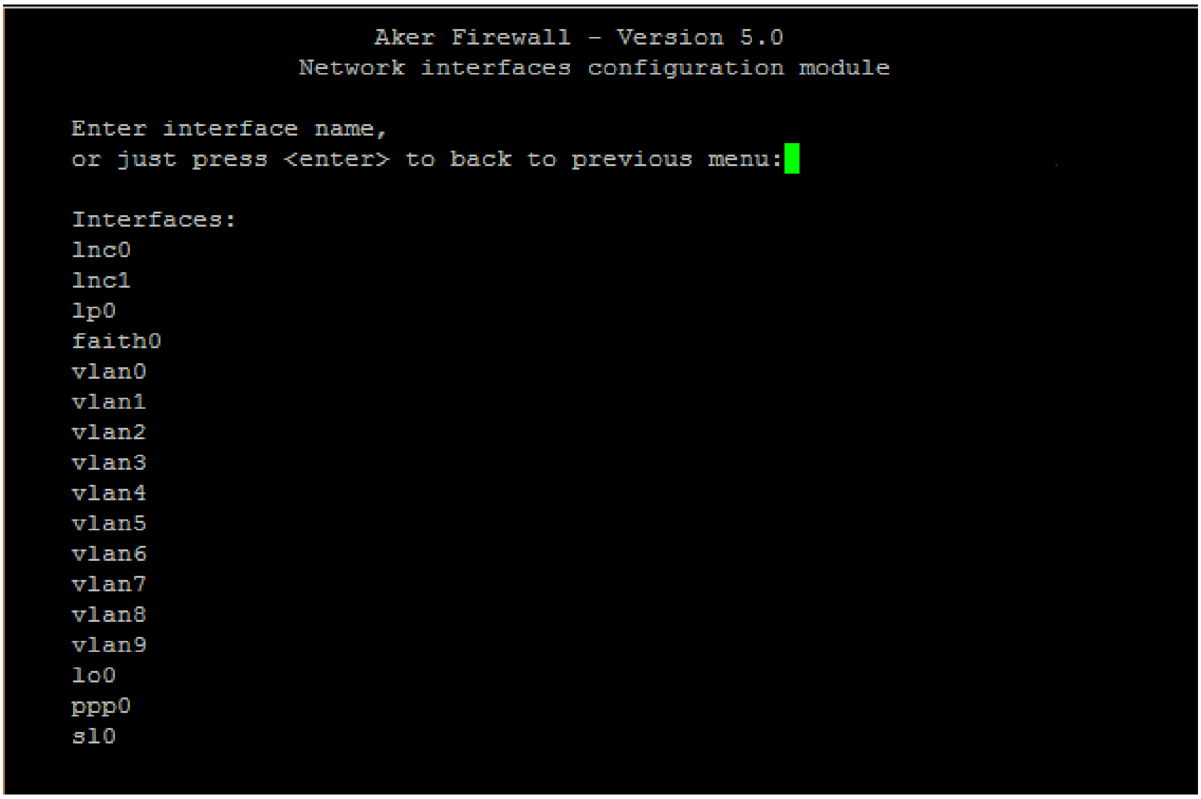
The screen below shows the List of network interfaces.



```
                      Aker Firewall - Version 5.0
                 Network interfaces configuration module
                        Network interfaces list

   Name          IP Address        Mask              Point-to-point Address

   lnc0          10.0.0.40         255.255.255.0
   lnc1          200.149.5.182     255.255.255.0
   lp0
   faith0
   vlan0
   vlan1
   vlan2
   vlan3
   vlan4
   vlan5
   vlan6
   vlan7
   vlan8
   vlan9
   lo0           127.0.0.1         255.0.0.0
   ppp0
   sl0


   Press any key to back to previous menu
```

Image – 542 Network Interface list.

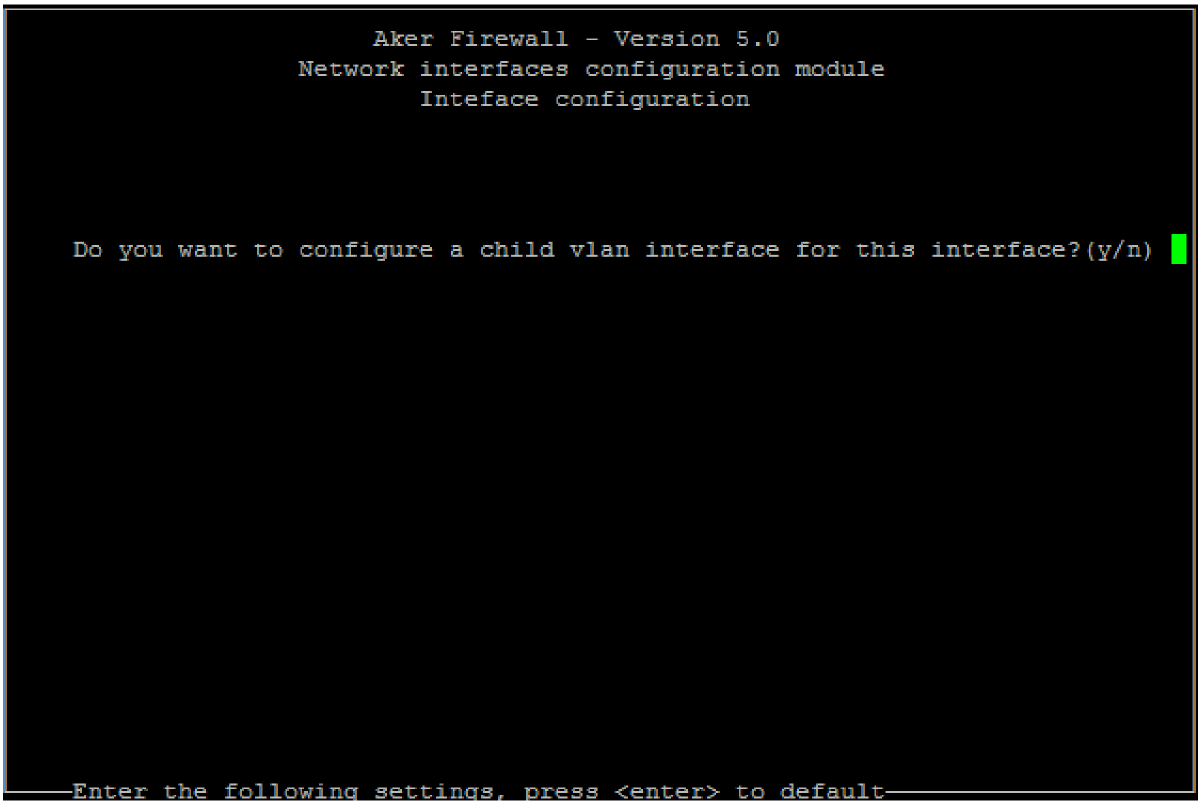
To configure an interface, just type its name. The <enter> key returns to the previous menu.



```
                        Aker Firewall - Version 5.0
                   Network interfaces configuration module

    Enter interface name,
    or just press <enter> to back to previous menu:

    Interfaces:
    lnc0
    lnc1
    lp0
    faith0
    vlan0
    vlan1
    vlan2
    vlan3
    vlan4
    vlan5
    vlan6
    vlan7
    vlan8
    vlan9
    lo0
    ppp0
    sl0
```

Image 543 – Network Interfaces configuration module

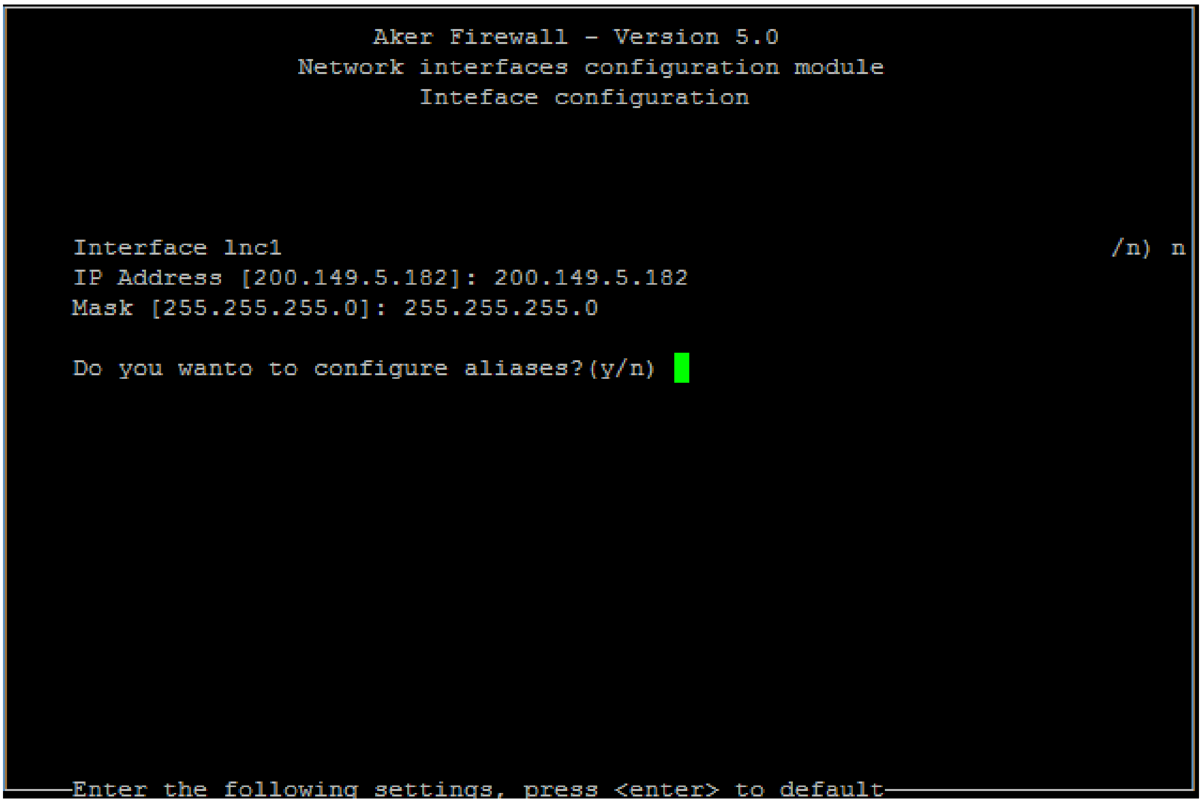
This screen shows the VLAN Registration option.



```
                Aker Firewall - Version 5.0
           Network interfaces configuration module
                 Inteface configuration



   Do you want to configure a child vlan interface for this interface?(y/n)

Enter the following settings, press <enter> to default
```

Image 544 – Vlan registration

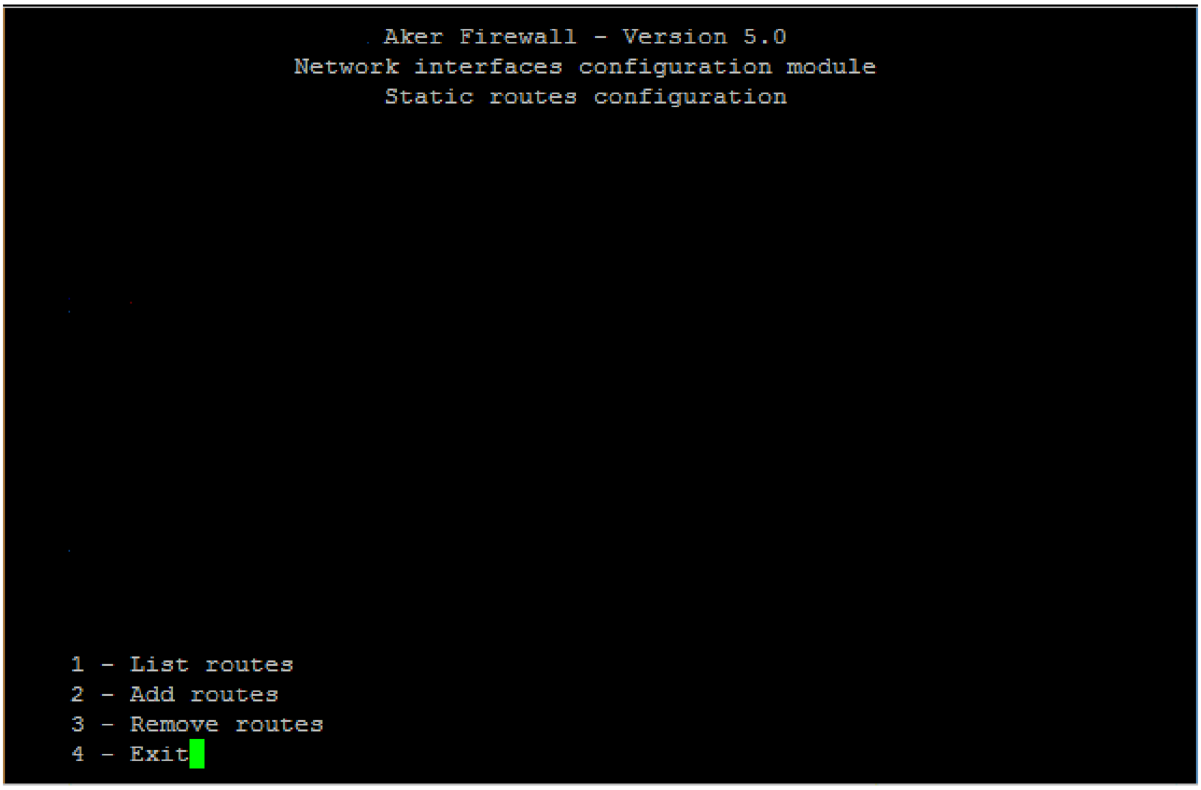
After configuration values are entered, it is possible to configure an *alias* for the interface.



```
                        Aker Firewall - Version 5.0
                   Network interfaces configuration module
                           Inteface configuration




    Interface lnc1                                                        /n) n
    IP Address [200.149.5.182]: 200.149.5.182
    Mask [255.255.255.0]: 255.255.255.0

    Do you wanto to configure aliases?(y/n)









    Enter the following settings, press <enter> to default
```

Image 545 – Interface configuration.

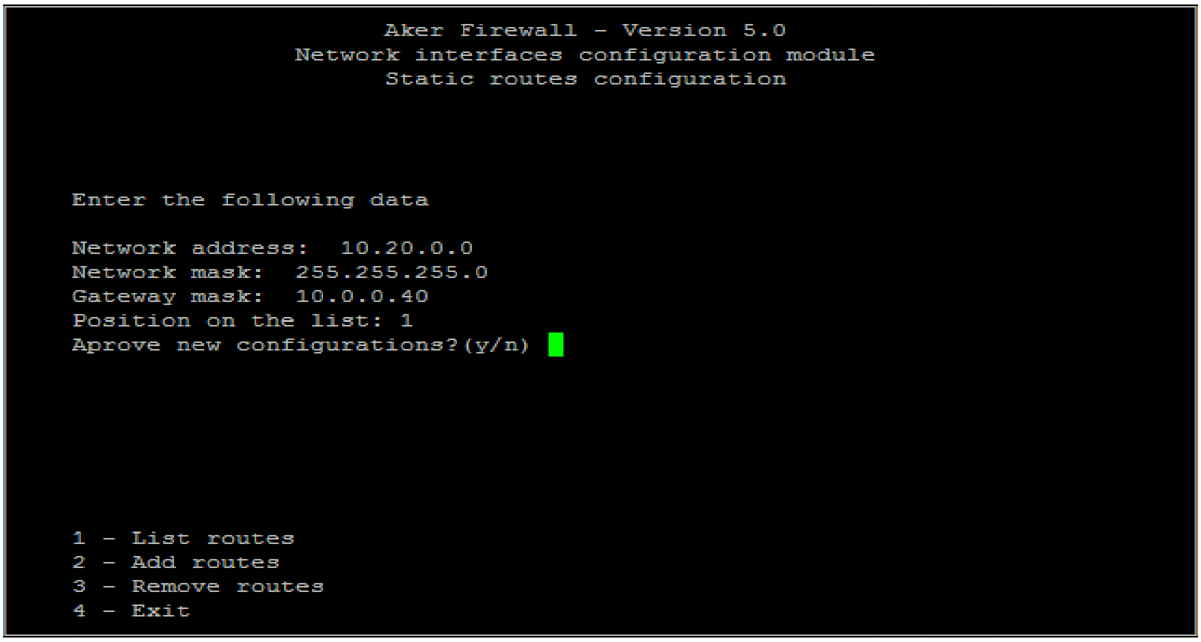
By choosing Option 2 in the main screen, it is possible to configure static routes.



```
                 Aker Firewall - Version 5.0
          Network interfaces configuration module
                Static routes configuration






    1 - List routes
    2 - Add routes
    3 - Remove routes
    4 - Exit
```

Image 546 – Static routes configuration.

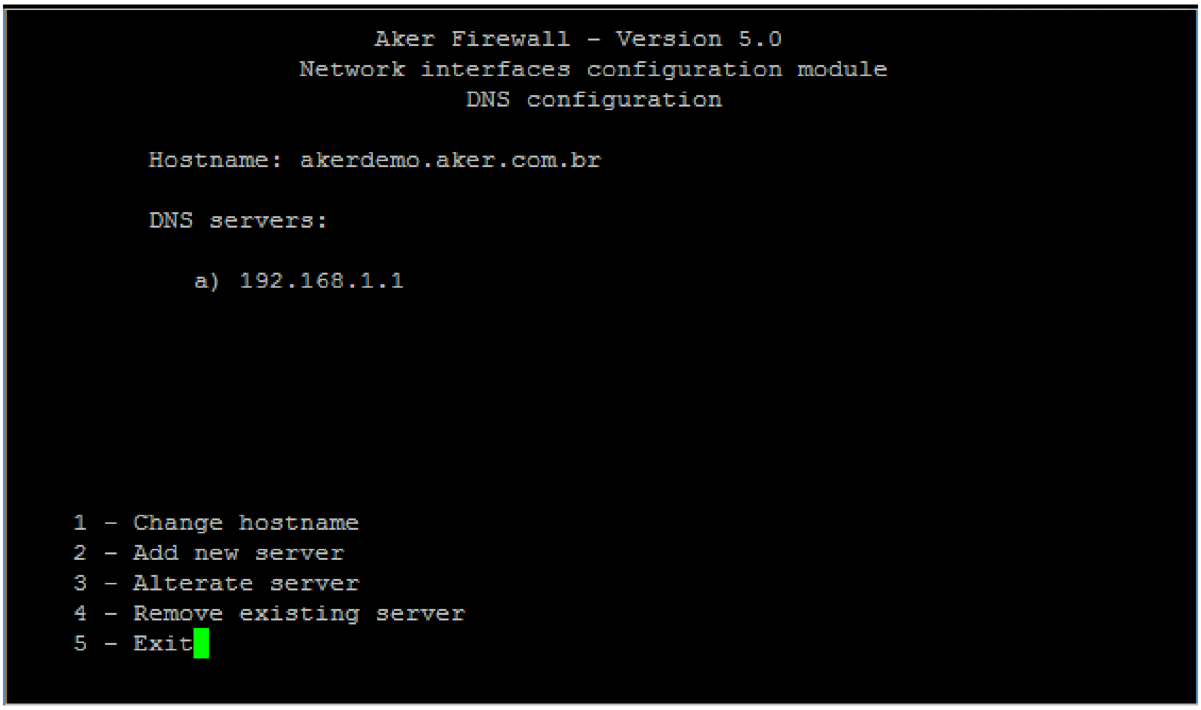
After the information has been entered, the program will request a confirmation to save the new configuration.



```
                         Aker Firewall - Version 5.0
                   Network interfaces configuration module
                         Static routes configuration




    Enter the following data

    Network address:  10.20.0.0
    Network mask:  255.255.255.0
    Gateway mask:  10.0.0.40
    Position on the list: 1
    Aprove new configurations?(y/n)






    1 - List routes
    2 - Add routes
    3 - Remove routes
    4 - Exit
```

Image 547 – Static routes configuration.

By choosing Option 3 in the main screen, it is possible to configure DNS Servers.

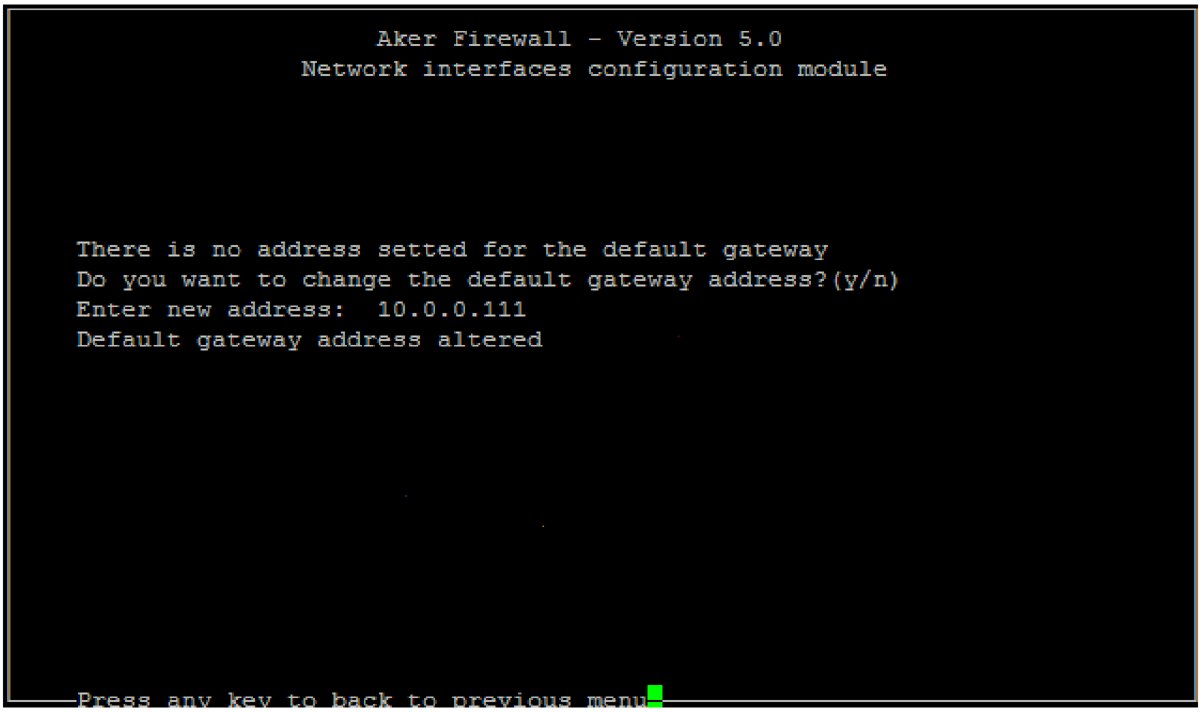


```
                        Aker Firewall - Version 5.0
                   Network interfaces configuration module
                              DNS configuration

         Hostname: akerdemo.aker.com.br

         DNS servers:

            a) 192.168.1.1





    1 - Change hostname
    2 - Add new server
    3 - Alterate server
    4 - Remove existing server
    5 - Exit
```

Image 548 – DNS configuration.

By choosing Option 4 in the main screen, it is possible to configure the default route.

Option 5 of the main screen saves the new configurations. If the user chooses Option 6, the firewall detects all modifications and asks if the user wants to exit without applying them.



```
                    Aker Firewall - Version 5.0
               Network interfaces configuration module




    There is no address setted for the default gateway
    Do you want to change the default gateway address?(y/n)
    Enter new address:  10.0.0.111
    Default gateway address altered









    Press any key to back to previous menu
```

Image 549 – Network Interfaces configuration module.

36.7. Using the text interface for Wireless configuration

This option is configured in the text interface and is available only for Aker Firewall Box with wireless connection support.

Aker Firewall has support to multiple SSID, so it is possible to meet different services, demands and transmitters.

To use multiple SSID on Aker firewall is required the creation of few interfaces with the following command:

Syntax: wireless create_interface ath0 ap g

Syntax: wireless create_interface ath1 ap g

Syntax: wireless create_interface ath...N ap g

The customized configuration shall be made for each new interface.

Below follows the Wireless configuration commands and few examples of configuration:

Program location: /aker/bin/firewall/akwireless

```
Usage: akwireless create_interface <interface> <sta|adhoc|ap|monitor|wds|ahdemo>
<b:g>

    akwireless destroy_interface <interface>

    akwireless change_protocol <interface> <b:g>

    akwireless list_interface [interface]

    akwireless change_mode <interface> <sta|adhoc|ap|monitor|wds|ahdemo>

    akwireless change_SSID <interface> <SSID>

    akwireless wep_key <interface> <index> <key>

    akwireless wep_key_index <interface> <index>

    akwireless wpa1_key <interface> <key> <file>

    akwireless wpa2_key <interface> <key> <file>

    akwireless no_key <interface>

    akwireless choose_mac_list <interface> black:white <mac_file>

    akwireless add_mac <interface> <mac>

    akwireless del_mac <interface> <mac>

    akwireless mac_list <interface>

    akwireless clear_list <interface>

    akwireless authentication_list |interface|

    akwireless change_channel <interface> |channel|

    akwireless list_connected_users <interface>
```

In a command containg the space signs "< >" (greater or less then) it is mandatory to insert the requested data. In case the space signs are "[ ]" (square brackets), it is not mandatory to insert any data.

Below follows some examples and explanation about the commands:

akwireless create_interface <interface> <sta | adhoc | ap | monitor | wds | ahdemo> <b:g> = creates an interface.

Syntax: *wireless create_interface ath0 ap g*

The most used mode is the "AP" (Modo Master) that allows other hosts connect to it.

There are several protocols such as A, B, G, N, however, **Aker Firewall** supports only B and G protocols on version 6.5 with patch or higher.

Wireless interfaces are known as "ath", in case there are 3 interfaces, they will be known as ath0, ath1 and ath2.

akwireless destroi_interface <interface> = destroys an interface.

Syntax: *wireless destroy_interface ath0*

akwireless change_protocol <inteface> <b:g> = changes the protocol that will be used.

Syntax: *wireless change_protocol ath0 g*

Note: Wireless card supports only one protocol for all interfaces.

akwireless list_interface [interface] = Lists all interfaces.

Syntax: *wireless list_interface*

If you wish to list a specific linterface, add its name infront of the command

e.g. *wireless list_interface test* (test is the interface name)

akwireless change_mode <interface> <sta | adhoc | ap | monitor | wds | ahdemo> = changes the mode that will be used.

Sintaxe: *wireless change_mode ath0 ap*

akwireless change_SSID <interface> <SSID> = create/change the wireless network name.

Syntax: *wireless change_SSID ath0 network1*

akwireless wep_key <interface> <index> <key> = enables the WEP authentication with the index and key indicated.

Syntax: wireless wep_key ath0 1 12345

akwireless wep_key_index <interface> <index> = changes current index.

Sintaxe: *wireless wep_key_index ath0 1*

You can create up to 4 distincs indexes.

akwireless wpa1_key <interface> <key> <file> = enables the WPA1 authentication with the key and configuration file indicated.

Syntax: *wireless wpa1_key ath0 123456789 wpa1.conf*

akwireless wpa2_key <interface> <key> <file> = enables the WPA2 authentication with the key and configuration file indicated.

Sintaxe: *wireless wpa2_key ath0 123456789 wpa2.conf*

akwireless no_key <interface> = disables the authentication.

Syntax: *wireless no_key ath0*

akwireless choose_mac_list <interface> black : white <mac_file> = enables MAC filtering.

Syntax: *wireless choose_mac_list ath0 white white.conf*

Black: list of macs that will not be allowed to connect to the Firewall.

White: list of macs that are allowed to connect to the Firewall.

akwireless add_mac <interface> <mac> = adds a mac to the list.

Syntax: *wireless add_mac ath0 00:13:20:3A:11:5B*

akwireless del_mac <interface> <mac> = deletes a mac from the list.

Syntax: *wireless del_mac ath0 00:13:20:3A:11:5B*

akwireless mac_list <interface> = show the list of macs.

Syntax: *wireless mac_list ath0*

akwireless clear_list <interface> = deletes all macs that have been listed.

Syntax: *wireless clear_list ath0*

akwireless authentication_list |interface| = lists the authentication type of each interface.

Syntax: *wireless authentication_list ath0*

akwireless change_channel <interface> |channel| = changes the interface channel.

Syntax: *wireless change_channel ath0 3*

To show all available channels simply use the command above without the indicating the channel.

e.g. *wireless change_channel*

a**kwireless list_connected_users** <interface> = shows connected users.

Syntax: *wireless list_connected_users ath0*

This configuration is performed only through the Text Interface..

36.8. Using the Text Interface for DDNS configuration

This option is configured in the text interface and is available only for Aker Firewall Box with wireless connection support.

Below follows the DDNS configuration commands and few examples of configuration:

***Program location**: /aker/bin/firewall/akddns*

akddns – Configures a DDNS client service

Usage: akddns [help | show | activate | deactivate | list | clear]

akddns interface <interface>

akddns server <servername> <service> <dynamic_name> [server_login] [pwd_server]

akddns gateway <gateway_type> <gateway_ip> <gateway_port> [gateway_login] [gateway_pwd]

akddns web <url> [token]

akddns ip <ip>

show = shows this message

activate = activates the DDNS client service

deactivate = deactivates the DDNS client service

show = shows the client current status and its configuration

list = lists the types of gateways that can be queried to get a public IP

server = configures the DDNS service that will be used

<servername> = DDNS service hostname

<service> = used service (example: dyndns2, zoneedit1)

<dynamic_name> = hostname that will be configured in the DDNS service

[server_login] = DDNS service login

[server_pwd] = DDNS service password

The DDNS client shall use one of the following commands to get the public IP of the configured hostname.

interface = uses interface's IP provided to the hostname that is being configured.

<interface> = interface name which has the used IP

gateway = query a gateway (router, etc) to get the public IP of the hostname that is being configured

<gateway_type> = type of gateway that will be queried (see command "list")

<gateway_ip> = gateway IP address

<gateway_port> = port where the query will be performed

[gateway_login] = gateway login

[gateway_pwd] = gateway password

web = query a WEB page that has the public IP for the hostname that is being configured

<url> = WEB page url that will be queried

[token] = Token which the query for the public IP will be performed

ip = establishes a static public IP for the hostname that is being configured

<ip> = static public IP address

In a command containg the space signs "< >" (greater or less then) it is mandatory to insert the requested data. In case the space signs are "[ ]" (square brackets), it is not mandatory to insert any data.

36.9. 3G link configuration

Aker Firewall brings to its clients two new features in the Internet access. Aker UTM solutions support 3G modems and Wireless networks.

This features have been developed with the purpose of provide greater mobility and ease in the Internet access.

Connection via 3G modem

Aker Firewall allows you to connect a 3G modem on your USB port and this connection shall be used as a link of data to access the Internet.

This way it provides users a greater economy, high performance and ease in the installation, because 3G links besides being cheaper and faster, they are also easy to be installed, not requiring any equipment, nor network cables.

36.10 Link aggregation

Link aggregation is a computer networking term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

Further terms are also used to describe the method including: port trunking, link bundling, Ethernet/network/NIC bonding, or NIC teaming.

The last standard launched by IEEE (Institute of Electrical and Electronic Engineers) is IEEE 802.1ax Aggregation Control Protocol (LACP) that deprecated the previous standard: IEEE 802.3ad.

Aggregation can be implemented at any of the lowest three layers of the OSI model. Commonplace examples of aggregation at layer 1 are power lines (e.g. IEEE 1901) and wireless (e.g. IEEE 802.11) network devices that combine multiple frequency bands into a single wider one. OSI layer 2 (data link layer, e.g. Ethernet frame in LANs or multi-link PPP in WANs, Ethernet MAC address) aggregation typically occurs across switch ports, which can be either physical ports, or virtual ones managed by an operating system, e.g. such as the ones of *Open vSwitch*. Aggregation is also possible at layer 3 in the OSI model, i.e. at the network layer (e.g. IP or IPX), using round-robin scheduling, or based on hash values computed from fields in the packet header, or a combination of these two methods. Regardless of the layer on which aggregation occurs, the network load is balanced across all links. Most methods provide failover/redundancy as well.

The following instructions will cover the most used link aggregation types covered by Aker Firewall. The following example will configure a bond interface (bond0) using two firewall Ethernet interface (eth0 and eth1).

```
#!/bin/bash

modprobe bonding mode=0 miimon=100 # load bonding module

ifconfig eth0 down   # putting down the eth0 interface
ifconfig eth1 down   # putting down the eth1 interface

ifconfig bond0 hw ether 00:11:22:33:44:55       # changing the MAC address of the bond0 interface
ifconfig bond0 192.168.55.55 up # to set ethX interfaces as slave the bond0 must have an ip.
```

It is possible to set up your bond interface according to your needs. Changing one parameter (mode=X) you can have the following bonding types:

mode=0   (balance-rr)

Round-robin policy: Transmit packets in sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.

mode=1 (active-backup)

Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance. The primary option affects the behavior of this mode.

mode=2 (balance-xor)

XOR policy: Transmit based on (source MAC address XOR'd with destination MAC address) modulo slave count. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.

mode=3 (broadcast)

Broadcast policy: transmits everything on all slave interfaces. This mode provides fault tolerance.

mode=4 (802.3ad)

IEEE 802.3ad Dynamic link aggregation: Creates aggregation groups that share the same speed and duplex settings. It uses all slaves in the active aggregator according to the 802.3ad specification.

mode=5 (balance-tlb)

Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

mode=6 (balance-alb)

Adaptive load balancing: includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.

The most used are the first four mode types...

Also you can use multiple bond interface but for that you must load the bonding module as many as you need.
Presuming that you want two bond interface you must configure the /etc/modules.conf as follow:

```
alias bond0 bonding
options bond0 -o bond0 mode=0 miimon=100
alias bond1 bonding
options bond1 -o bond1 mode=1 miimon=100
```

Notes:

To restore your slaves MAC addresses, you need to detach them from the bond (`ifenslave -d bond0 eth0'). The bonding driver will then restore the MAC addresses that the slaves had before they were enslaved.

The bond MAC address will be the taken from its first slave device.

Promiscous mode: According to your bond type, when you put the bond interface in the promiscous mode it will propogates the setting to the slave devices as follow:

for mode=0,2,3 and 4 the promiscuous mode setting is propogated to all slaves.

for mode=1,5 and 6 the promiscuous mode setting is propogated only to the active slave.

For balance-tlb mode the active slave is the slave currently receiving inbound traffic, for balance-alb mode the active slave is the slave used as a "primary." and for the active-backup, balance-tlb and balance-alb modes, when the active slave changes (e.g., due to a link failure), the promiscuous setting will be propogated to the new active slave.

Configuring the Firewall in Cluster

37. Configuring the firewall in Cluster

This chapter shows how to configure the fault-tolerance and the cooperative cluster of Aker Firewall.

37.1. Planning the installation

What is a Fault-tolerant system?

Fault-tolerance or **graceful degradation** is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naïvely-designed system in which even a small failure can cause total breakdown. Fault-tolerance is particularly sought-after in high-availability or life-critical systems.

Fault-tolerance is not just a property of individual machines; it may also characterize the rules by which they interact. For example, the Transmission Control Protocol (TCP) is designed to allow reliable two-way communication in a packet-switched network, even in the presence of communications links which are imperfect or overloaded. It does this by requiring the endpoints of the communication to *expect* packet loss, duplication, reordering and corruption, so that these conditions do not damage data integrity, and only reduce throughput by a proportional amount.

Data formats may also be designed to degrade gracefully. HTML for example, is designed to be forward compatible, allowing new HTML entities to be ignored by Web browsers which do not understand them without causing the document to be unusable.

Recovery from errors in fault-tolerant systems can be characterized as either **roll-forward** or **roll-back**. When the system detects that it has made an error, roll-forward recovery takes the system state at that time and corrects it, to be able to move forward. Roll-back recovery reverts the system state back to some earlier, correct version, for example using check pointing, and moves forward from there. Roll-back recovery requires that the operations between the checkpoint and the detected erroneous state can be made idempotent. Some systems make use of both roll-forward and roll-back recovery for different errors or different parts of one error.

Within the scope of an *individual* system, fault-tolerance can be achieved by anticipating exceptional conditions and building the system to cope with them, and, in general, aiming for self-stabilization so that the system converges towards an error-free state. However, if the consequences of a system failure are catastrophic, or the cost of making it sufficiently reliable is very high, a better solution may be to use some form of duplication. In any case, if the consequence of a system failure is so catastrophic, the system must be able to use reversion to fall back to a safe mode. This is similar to roll-back recovery but can be a human action if humans are present in the loop.

What is a cooperative system?

A cooperative system is defined to be a system of multiple dynamic entities that share information or tasks to accomplish a common, though perhaps not singular, objective. Examples of cooperative control systems might include robots operating within a manufacturing cell, unmanned aircraft in search-and-rescue operations or military surveillance and attack missions, arrays of micro satellites that form a large distributed aperture radar, employees operating within an organization, and software agents. The term "entity" is most often associated with vehicles capable of physical motion, such as robots, automobiles, ships, and aircraft, but the definition extends to any entity concept that exhibits a time-dependent behavior. Critical to cooperation is communication, which may be accomplished through active message passing or by passive observation. It is assumed that cooperation is being used to accomplish some common purpose that is greater than the purpose of each individual, but also recognized that the individual may have other objectives as well, perhaps due to being a member of other caucuses. This implies that cooperation may assume hierarchical forms. The decision-making process (i.e., the control) is typically distributed or decentralized to some degree. For, if not, a cooperative system could always be modeled as a single entity. The level of cooperation may be indicated by the amount of information exchanged between entities. Cooperative systems may involve task sharing and can consist of heterogeneous systems if they are composed of humans and machines. Finally, one is often interested in how cooperative systems perform under noisy or adversary conditions.

How does Aker Firewall fault tolerance work?

Aker Firewall fault tolerance is composed of two identical systems, i.e. two hosts with the same operating system, same network adapter and same Firewall version, connected to each other. The requirement to use the same operating system is necessary because when applying corrections through the Remote Interface (control Center) in one host, will be automatically replicated in the other.

Besides the hosts be connected to each other, which is done by on network interface it is required that all network adapters corresponding to the hosts be connected to a Hub or Switch, so both firewalls can have access to the same hosts and routers.

How does Aker Firewall cooperative system work?

First of all the basic difference between the cooperative cluster and the failover is linked to the license. The cooperative cluster causes the convergence of two firewalls with the same weight be 50% for each, and the failover license makes the convergence in only one of the firewalls.

What are UNICAST and MULTICAST modes of Aker Firewall cooperative system?

On Aker Firewall in cooperative mode, more than one host (Cluster nodes) need receive the same packets, so later each one of them can decide if these packets are or not the host’s responsibility. As the switches are not natively prepared, one of the following techniques (UNICAST or MULTICAST) needs to be used.

The first technique is known as UNICAST, it reconfigures the switch so it can be able to know that a specific Ethernet address (MAC) is in more than two ports simultaneously meaning that the switch needs to copy the packet with this destination address in all ports, and never hold it as it is in one port only. In this mode, all cluster’s firewalls use the same MAC address. The only problem of this mode is; only few switches support this operation.

The second technique is knows as MULTICAST, it makes the cluster’s firewalls register a multicast Ethernet address in their interfaces and respond to *ARP request* to the Virtual IP with this address. If the switch does not be configured to limit the spreading of multicast packets, all packets sent to the firewall will be redistributed in all ports, as they were broadcast packets.

To perform this configuration there are two options: manually on the switch, or use an IGMP protocol, where each firewall announces to the switch that it is a member of a multicast group corresponding to the chosen address. There are some routers that do not learn the multicast Ethernet address from the *ARP reply* sent by the firewall, in these cases the entries to the firewall shall be added manually in its table.

There are serious implications of performance (e.g. flooding) and security (IGMP association request) in case of cluster in multicast mode. All problems can be avoided by configuring the switches correctly.

When the cluster is active, any change on the firewall configuration through the Remote Interface will be applied automatically to the other firewall.

37.2. Cluster configuration

In order to start the cluster configuration, it is necessary that a cluster license be previously applied to the firewall.

To gain access to the Cluster configuration window, follow the steps below:

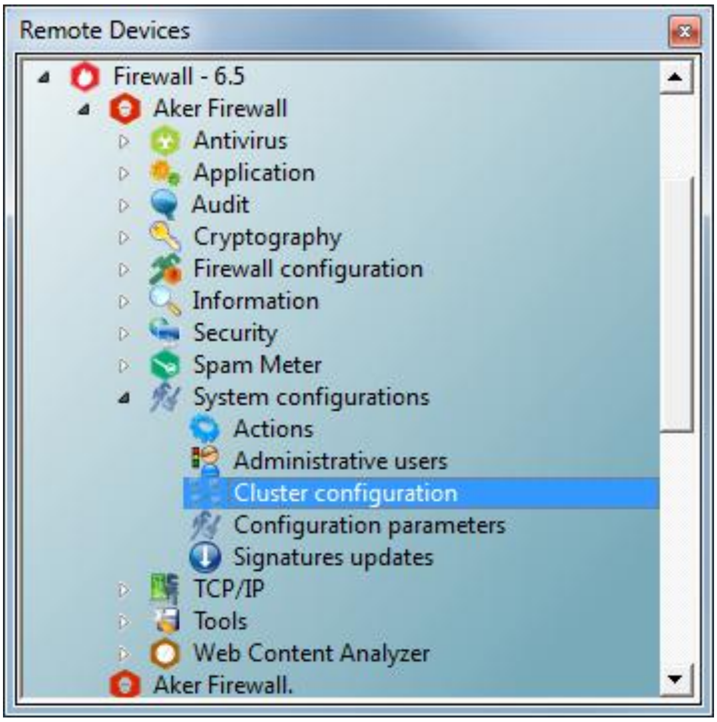
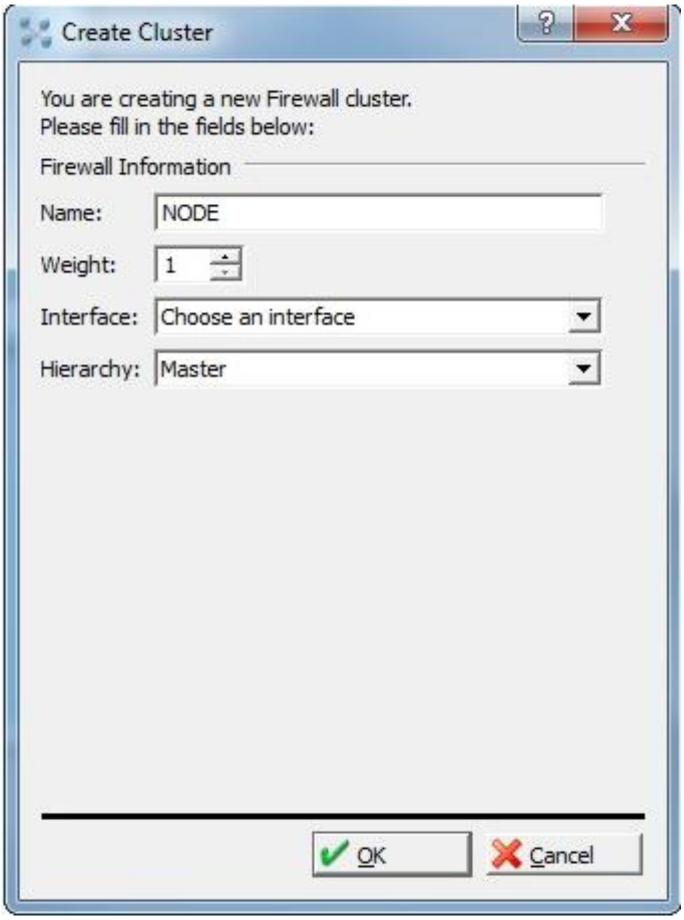

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
Actions
Administrative users
Cluster configuration
Configuration parameters
Signatures updates
TCP/IP
Tools
Web Content Analyzer
Aker Firewall.

Image 554 – Access window: Cluster configuration

- Click on the *System configurations* menu.
- Select *Cluster configuration*.

In case the user chooses the option configure the cluster click on “YES”, and the following screen will be displayed:



You are creating a new Firewall cluster.
Please fill in the fields below:

Firewall Information

Name: NODE

Weight: 1

Interface: Choose an interface

Hierarchy: Master

Image 555 – Create cluster

This window allows creating a new cluster. The following fields need to be filled in:

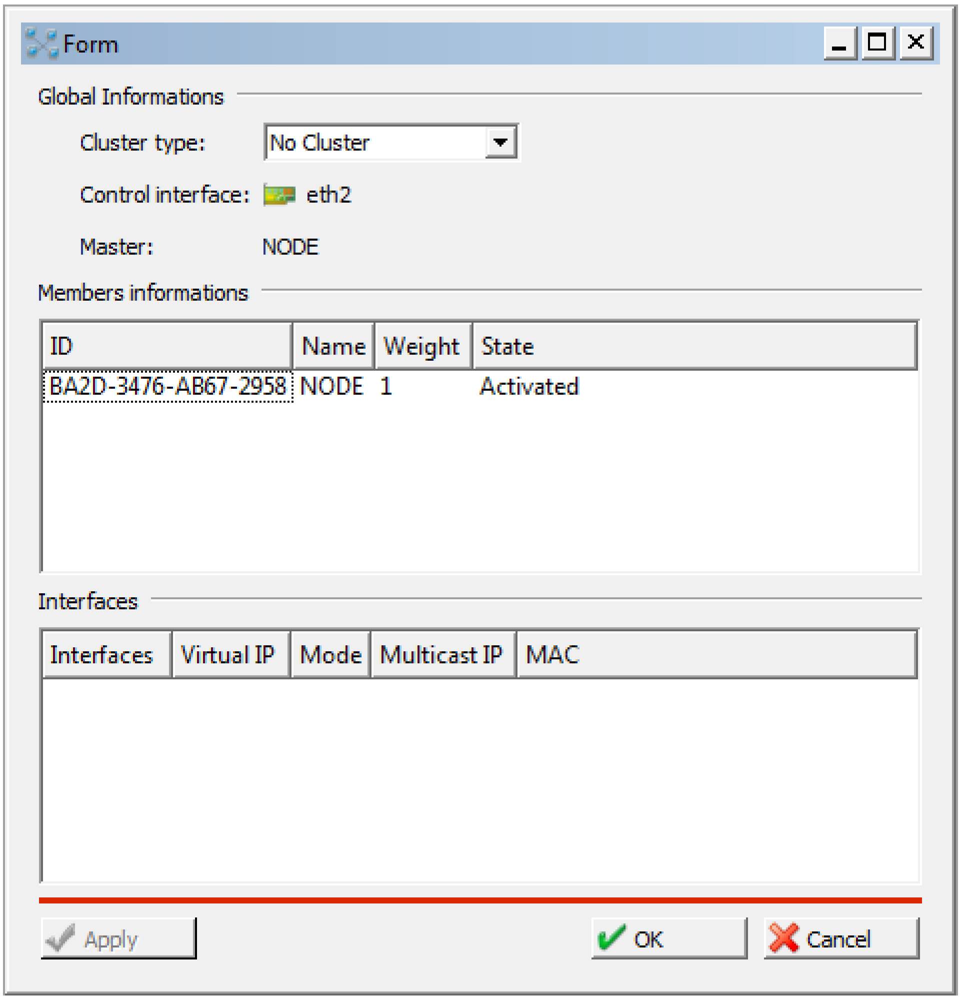
Name: Firewall name in the cluster.

Weight: This field indicates the traffic load balancing. The administrator shall choose the most appropriate value.

Interface: In this field you will choose an entity that will represent a Firewall Control Interface. This entity will be used by the firewall to control the cluster.

If the cluster creation has been made successfully, the Remote Interface (Control Center) will be disconnected to ensure that the entire configuration of the firewall reloaded.

In case you wish to make any change on the configurations of the cluster that has been created, access the Cluster configuration window. Below follows the description of each field:



Global Informations

Cluster type: No Cluster

Control interface: eth2

Master: NODE

Members informations

ID	Name	Weight	State
BA2D-3476-AB67-2958	NODE	1	Activated

Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC

Image 556 – Cluster configuration – Global Information

Global Information

In this window the global information of the created cluster will be displayed.

Cluster type: This option selects the desired type of cluster or disables it.

Control interface: This information is set when you are creating the cluster and CANNOT be changed later.

Members' information

This area shows all information about the cluster members.

Identification: This field informs the cluster's ID. It is randomly generated and cannot be changed.

Name: Indicates the cluster firewall name.

Weight: This field indicates the traffic load balancing. The administrator shall choose the most appropriate value.

State: Allows you to view the cluster status which might be “Activated” or “Deactivated”.

Interfaces

This part of the windows displays the network interfaces configuration features of cluster’s members. These features belongs to all members, activated, deactivated, and the ones that will be included.

Interface: In this part the new interfaces will be added.

Virtual IP: Represents the cluster’s hosts for the current network. It shall be set only for cooperative cluster.

Mode: Chooses the mode that the packets will be redistributed within a host group. The default is UNICAST, but can be changed to MULTICAST or MULTICAST (IGMP).

Multicast IP: The information in this field is changed according to the chosen mode, but it can be edited only for Multicast (IGMP).

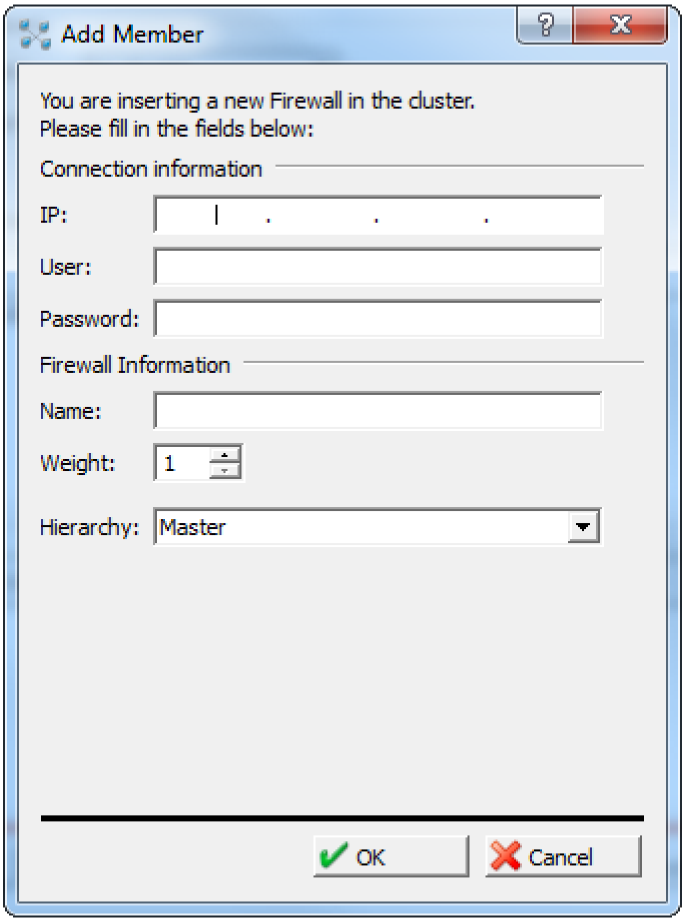
MAC: This field indicates the network adapter physical address. It is informed when the Multicast mode is selected. Not specifying the cluster, the network adapter address will be used, and if the Multicast (IGMP) mode is selected MAC will not be configured.

The add Virtual IP option is available only for cooperative cluster.

Note: There must be at least one active member.

Adding a new member

In this window you will be able to add a new member of the cluster. To add a new member click on the add member button which is located on the toolbar, and the following window will be displayed:



You are inserting a new Firewall in the cluster.
Please fill in the fields below:

Connection information

IP: . . .

User:

Password:

Firewall Information

Name:

Weight: 1

Hierarchy: Master

Image 557 – Cluster configuration: Add Member

In this window all information about the firewall that will be added to the cluster shall be filled in. Below follows the description of the fields:

Connection information

IP: Control Interface IP address where the cluster will be added.

User: Firewall administrator.

Password: Firewall administrator password.

Firewall Information

Name: Firewall name in the cluster

Weight: This field indicates the traffic load balancing. The administrator shall choose the most appropriate value.

Hierarchy: Sets the cluster status in master, slave or none.

- Master: Active host that will treat all requests.
- Slave: A node that will be activated only if the Master station is down.

- None: Hosts will decide among themselves which station will be master or slave.

37.3. Cluster statistics

The Cluster statistics window allows you to view the information of each node in the cluster.

To gain access to the Cluster statistics configuration window follow the steps below:

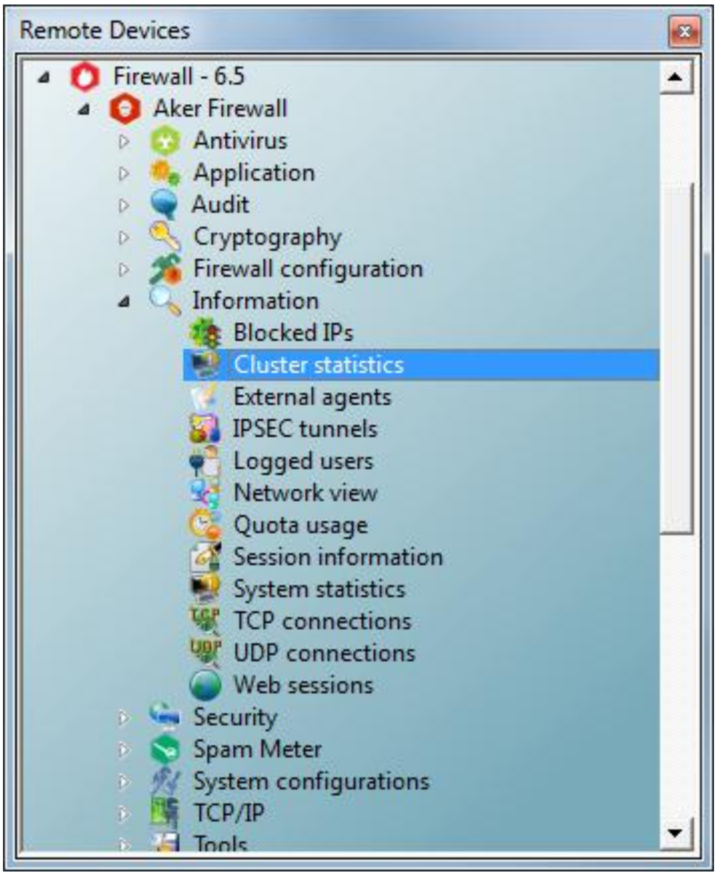
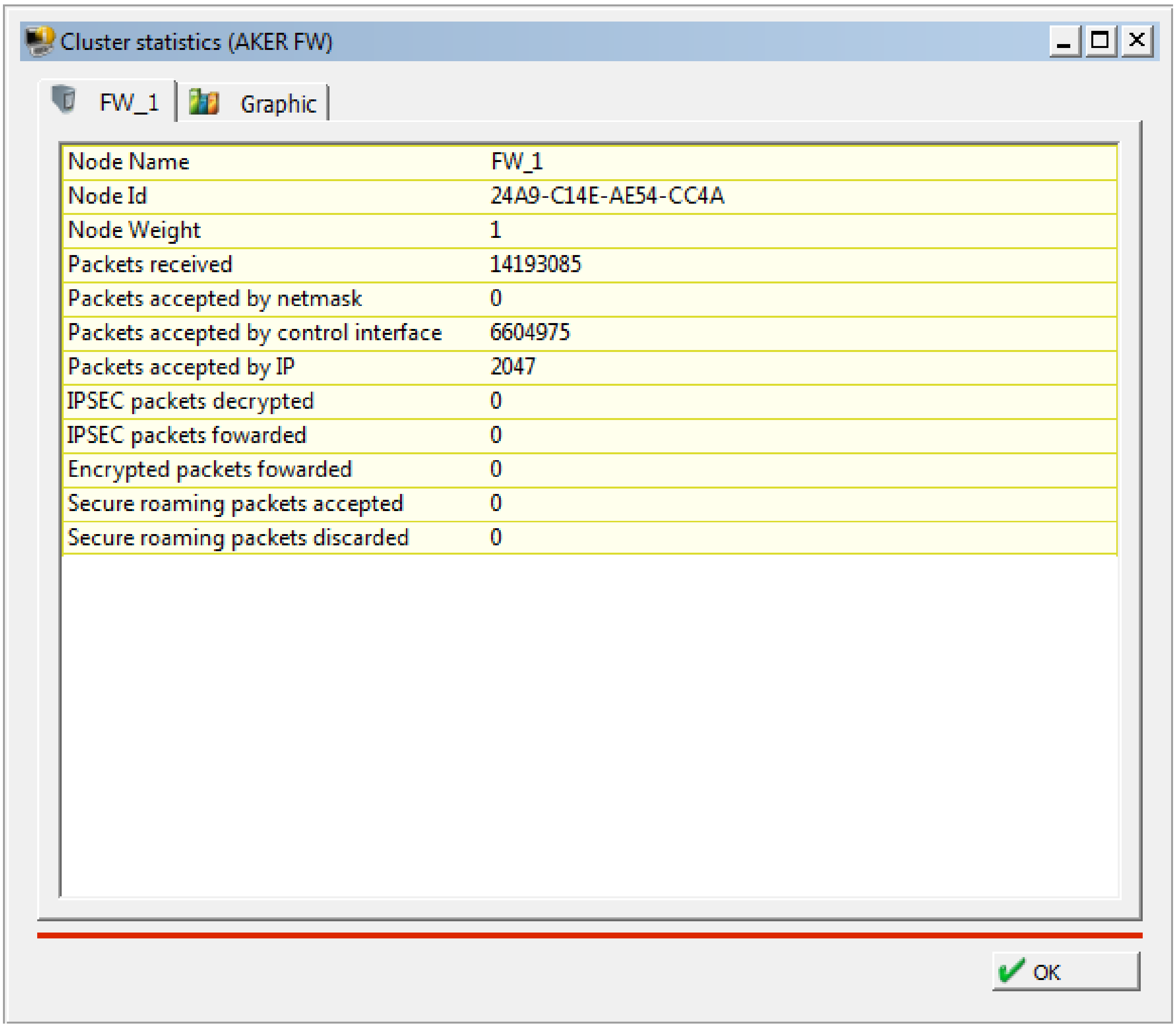

Remote Devices
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Blocked IPs
Cluster statistics
External agents
IPSEC tunnels
Logged users
Network view
Quota usage
Session information
System statistics
TCP connections
UDP connections
Web sessions
Security
Spam Meter
System configurations
TCP/IP
Tools

Image 558 – Access window: Cluster statistics.

- Click on the *Informaiton* menu
- Select *Cluster statistics*.

FW_1 tab

In this window you will find information about the cluster.



Node Name	FW_1
Node Id	24A9-C14E-AE54-CC4A
Node Weight	1
Packets received	14193085
Packets accepted by netmask	0
Packets accepted by control interface	6604975
Packets accepted by IP	2047
IPSEC packets decrypted	0
IPSEC packets fowarded	0
Encrypted packets fowarded	0
Secure roaming packets accepted	0
Secure roaming packets discarded	0

Image 559 – Cluster statistics: NODE.

Graphic tab

In this window you will see the information about the treatment given to the packets of nodes that pass through the firewall. This graphic allows viewing up to 8 nodes.

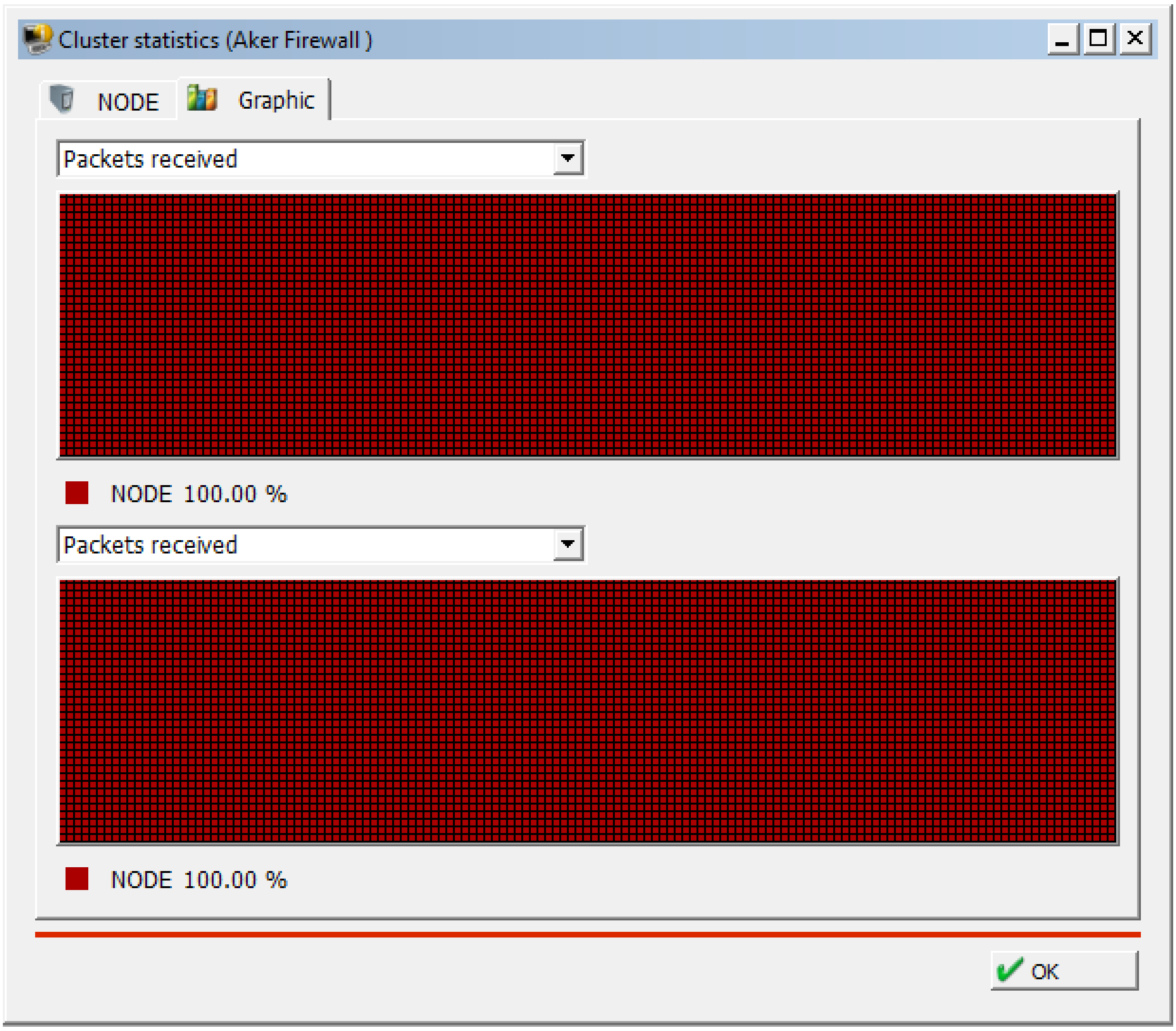

Cluster statistics (Aker Firewall)
NODE
Graphic
Packets received
🟥 NODE 100.00 %
Packets received
🟥 NODE 100.00 %
OK

Image 560 – Cluster statistic: Graphic

37.4. Configuring the cooperative cluster

To begin a Cooperative cluster configuration on Aker Firewall, is required that the licenses are applied, TCP/IP connections made, and all interfaces registered.

To configure a cooperative cluster follow the steps below:

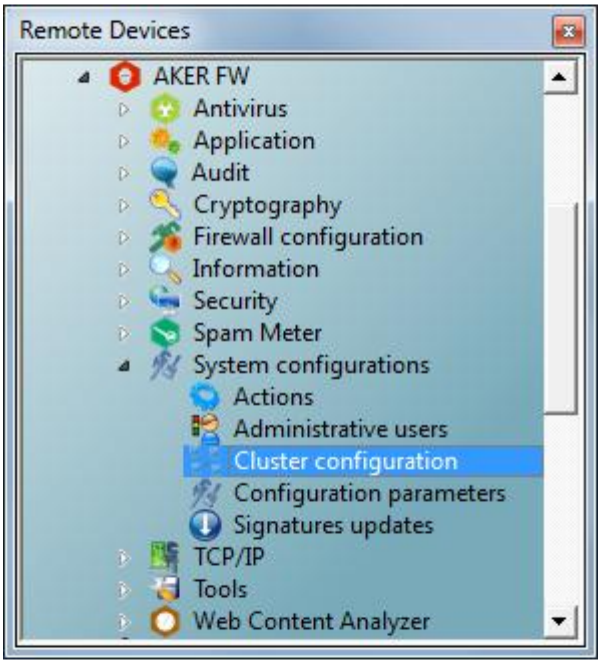
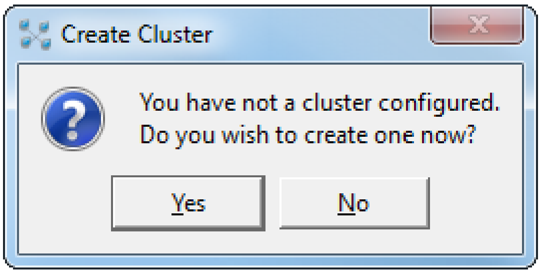

Remote Devices
AKER FW
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
Actions
Administrative users
Cluster configuration
Configuration parameters
Signatures updates
TCP/IP
Tools
Web Content Analyzer

Image 561 – Access window: Cluster configuration.

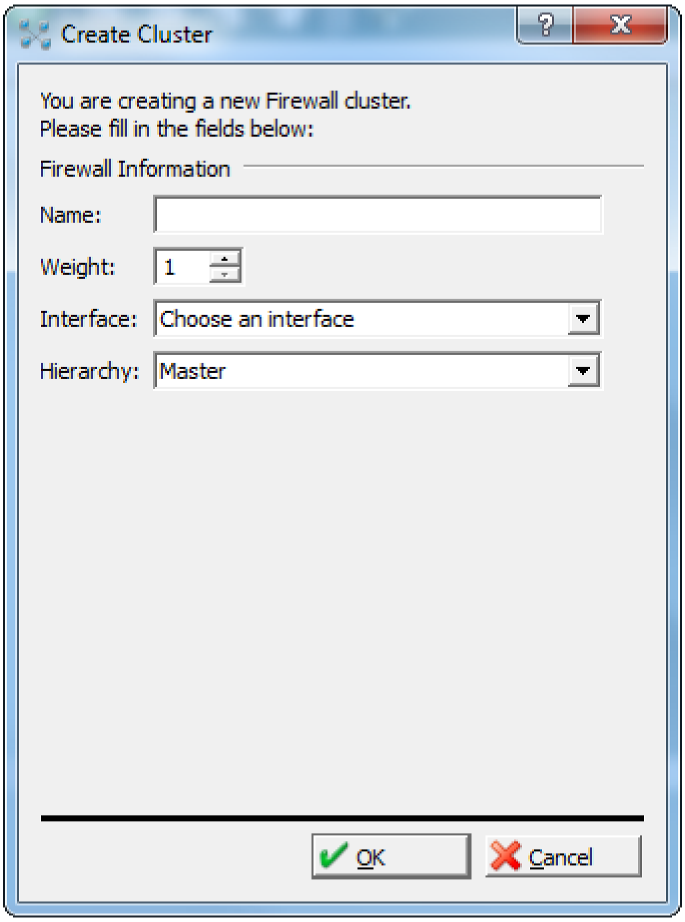
- Click on the *System configurations*
- Select *Cluster configuration*


Create Cluster
Yes
No

You have not a cluster configured.
Do you wish to create one now?

Image 562 – Create Cluster.

Selecting the option **Yes**, a new window will be displayed:



You are creating a new Firewall cluster.
Please fill in the fields below:

Firewall Information

Name:

Weight: 1

Interface: Choose an interface

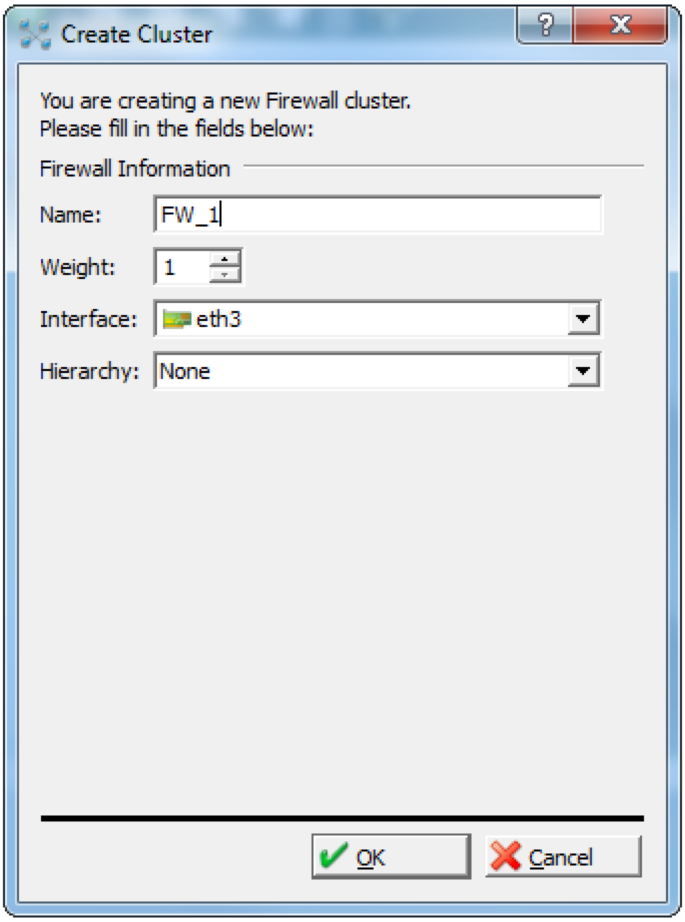
Hierarchy: Master

Image 563 – Filling out the fields to create a cluster.

The following fields must to be filled in:

- **Name:** Equipment name;
- **Weight:** This field indicates the traffic load balancing. The administrator shall choose the most appropriate value.
- **Interface:** In this field you will choose an entity that will represent a Firewall Control Interface. This entity will be used by the firewall to control the cluster.
- **Hierarchy:** Select the option **NONE.**

Below follows an example of configuration:



You are creating a new Firewall cluster.
Please fill in the fields below:

Firewall Information

Name: FW_1

Weight: 1

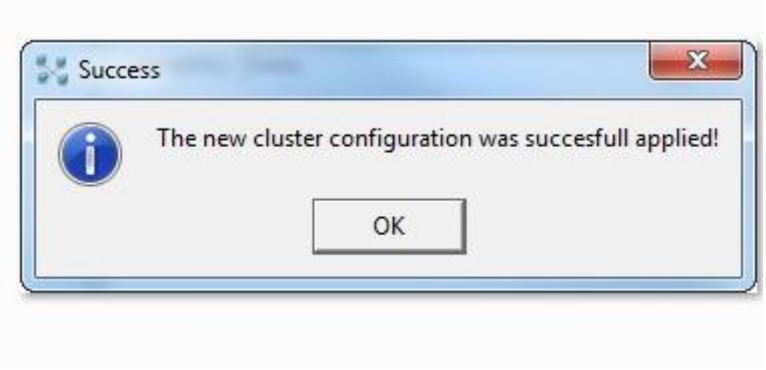
Interface: eth3

Hierarchy: None

Image 564 – Example

After filling all fields click on the **“OK”** button**.**

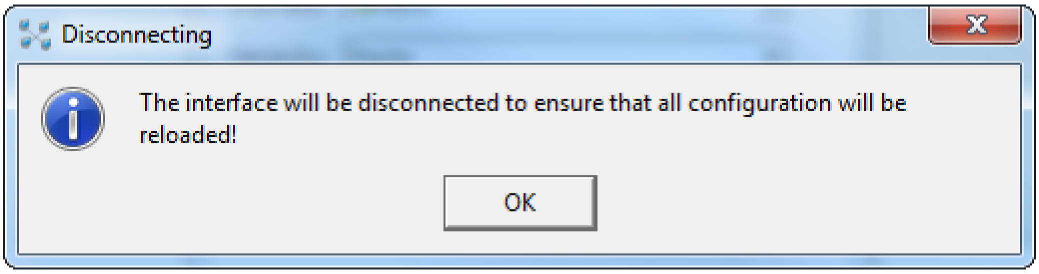
A new window will be displayed with the following message: **“The new cluster configuration has been successfully applied!”**.



The new cluster configuration was succesfull applied!

Image 565 – Cluster configuration has been successfully applied

Following you will be disconnected to ensure that all configurations will be reloaded.

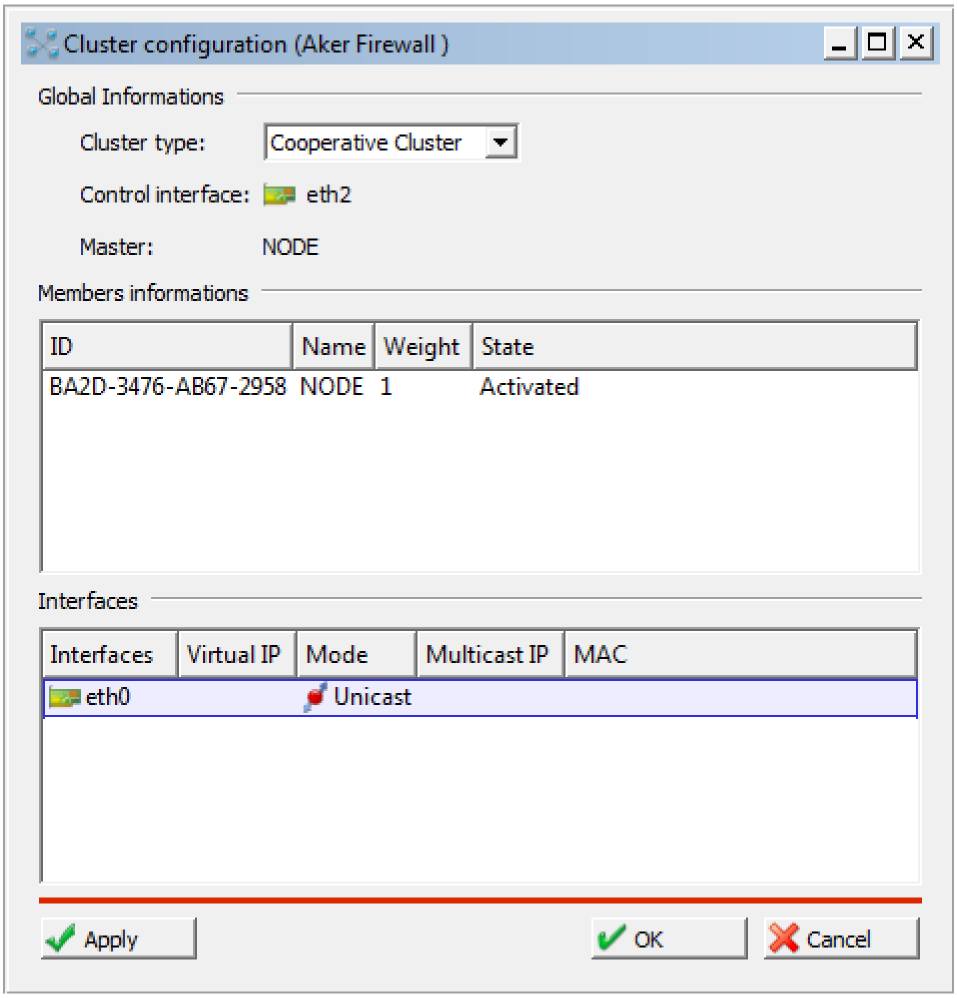


The interface will be disconnected to ensure that all configuration will be reloaded!

Image 566 – Disconnecting message

Open the control center again and follow the steps bellow:

- Click on the *System configurations*
- Select *Cluster configuration*
- On the *cluster type* option select “*Cooperative Cluster*”



Cluster configuration (Aker Firewall)

Global Informations

Cluster type: Cooperative Cluster

Control interface: eth2

Master: NODE

Members informations

ID	Name	Weight	State
BA2D-3476-AB67-2958	NODE	1	Activated

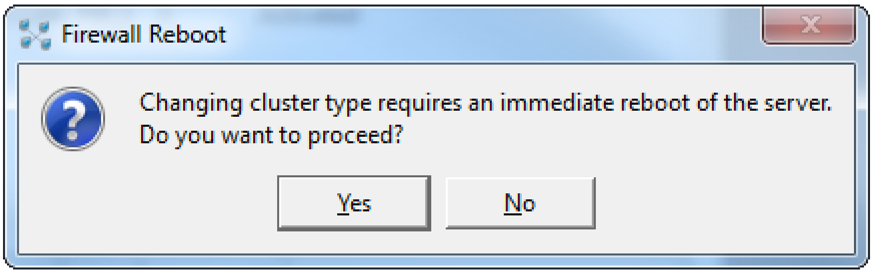
Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0		Unicast		

Apply
OK
Cancel

Image 567 – Cooperative Cluster

A new window will be displayed request to reboot the server.



Firewall Reboot

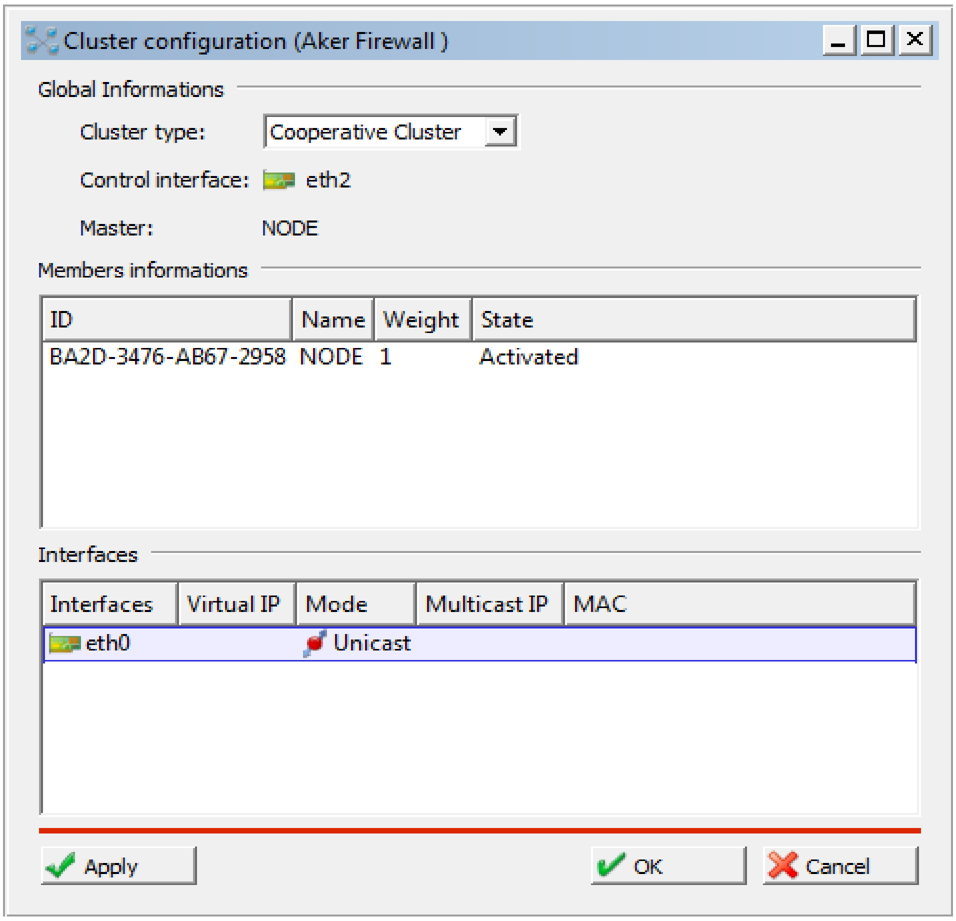
Changing cluster type requires an immediate reboot of the server.
Do you want to proceed?

Image 568 – Firewall Reboot message.

Click on **YES** and wait until the server is restarted.

Open the control center again and follow the steps bellow:

- Click on the *System configurations*
- Select *Cluster configuration*
- On the *Interface blank area right-click and add registered interfaces as the Image below:*



Cluster configuration (Aker Firewall)

Global Informations

Cluster type: Cooperative Cluster

Control interface: eth2

Master: NODE

Members informations

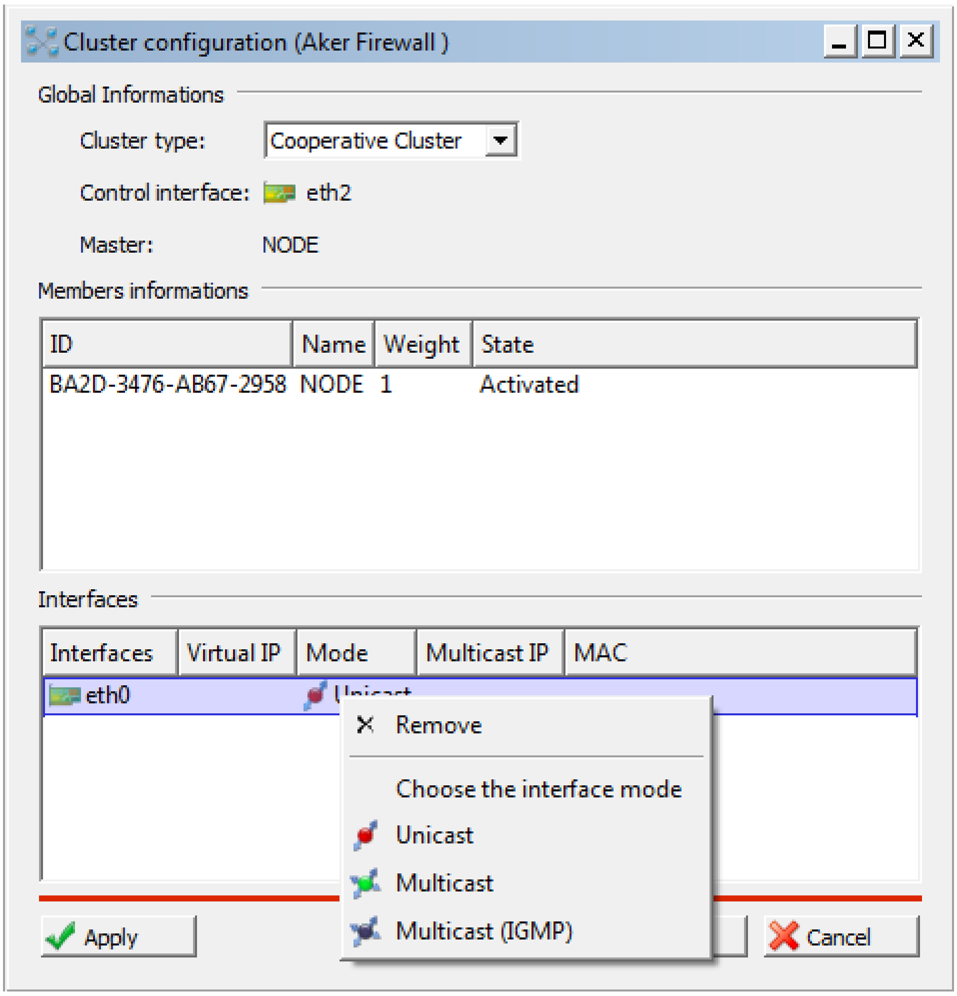
ID	Name	Weight	State
BA2D-3476-AB67-2958	NODE	1	Activated

Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0		Unicast		

Image 569 – Cluster Configuration

Right-click on one of the registered interfaces and select the option **Multicast**:



Cluster configuration (Aker Firewall)

Global Informations

Cluster type: Cooperative Cluster

Control interface: eth2

Master: NODE

Members informations

ID	Name	Weight	State
BA2D-3476-AB67-2958	NODE	1	Activated

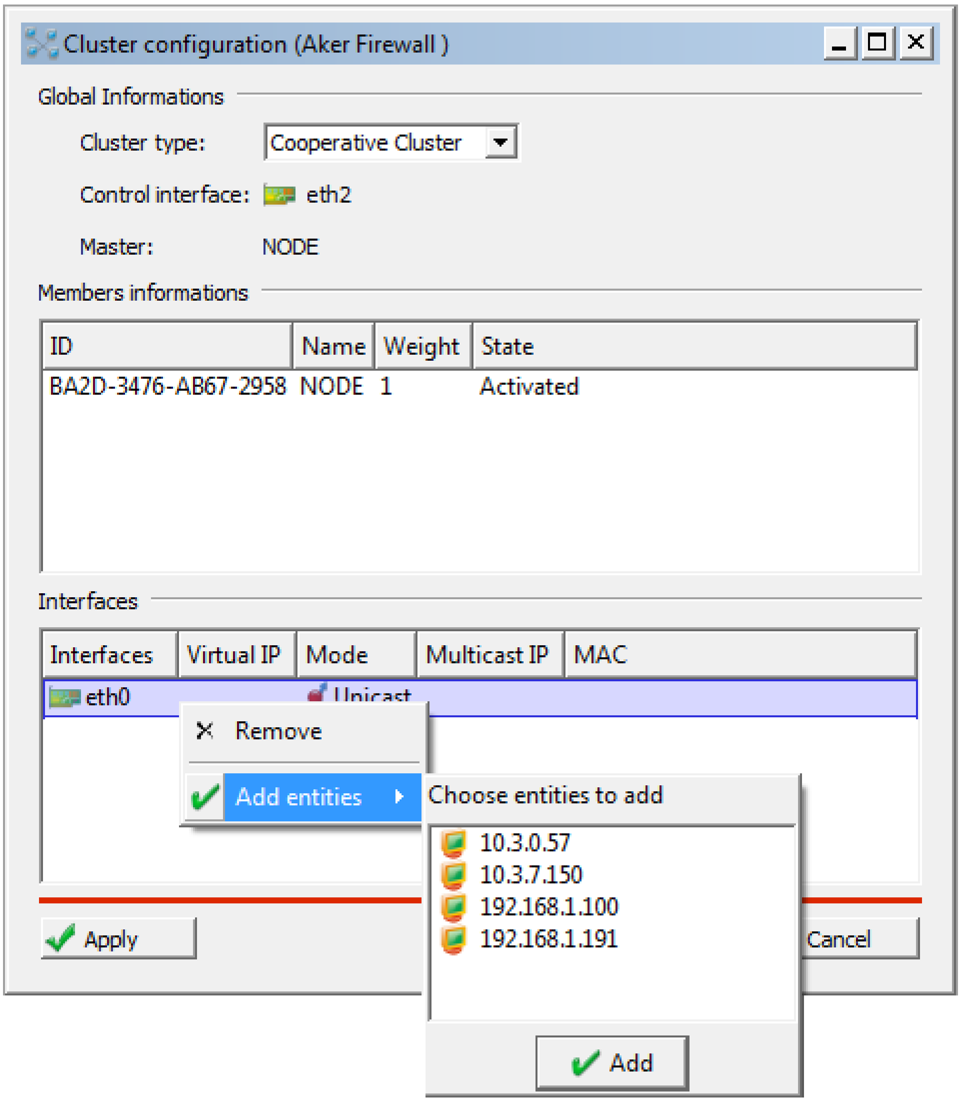
Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0		Unicast		

Remove
Choose the interface mode
Unicast
Multicast
Multicast (IGMP)
Apply
Cancel

Image 570 – Choosing the mode

Now right-click on the Virtual IP column and add the entity which the network adapter is being configured:


Cluster configuration (Aker Firewall)
Global Informations
Cluster type:
Cooperative Cluster
Control interface:
eth2
Master:
NODE
Members informations
Interfaces
Remove
Add entities
Choose entities to add
Add
Apply
Cancel

ID	Name	Weight	State
BA2D-3476-AB67-2958	NODE	1	Activated

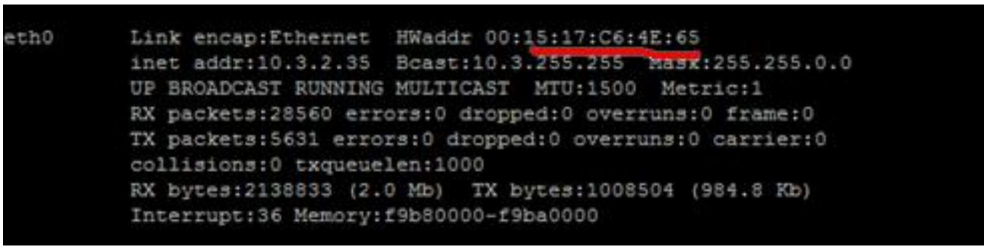
Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0		Unicast		

10.3.0.57
10.3.7.150
192.168.1.100
192.168.1.191

Image 571 – Adding entities.

After the procedure above, access the Text Interface using the command “ifconfig”

Copy the mac address of the interface you are using on the cluster configuration.



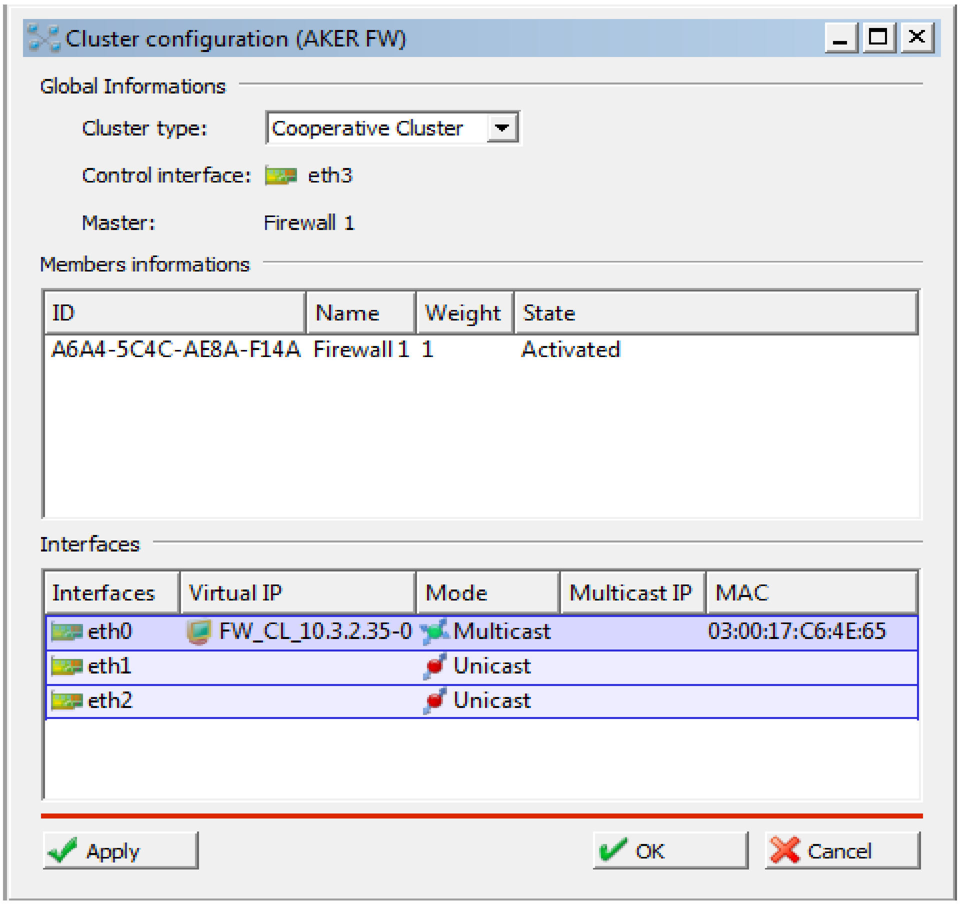
```
eth0      Link encap:Ethernet  HWaddr 00:15:17:C6:4E:65
          inet addr:10.3.2.35  Bcast:10.3.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28560 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5631 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2138833 (2.0 Mb)  TX bytes:1008504 (984.8 Kb)
          Interrupt:36 Memory:f9b80000-f9ba0000
```

Image 572 – Accessing the Text Interface

Copy the last 4 MAC address octets of the interface you are using in this example *17:C6:4E:65,* to register in the cluster configuration

Open the control center again and follow the steps bellow:

- Click on the *System configurations*
- Select *Cluster configuration*
- On Interface click on MAC and add the last 4 mac address octets as the example below:



Cluster configuration (AKER FW)

Global Informations

Cluster type: Cooperative Cluster

Control interface: eth3

Master: Firewall 1

Members informations

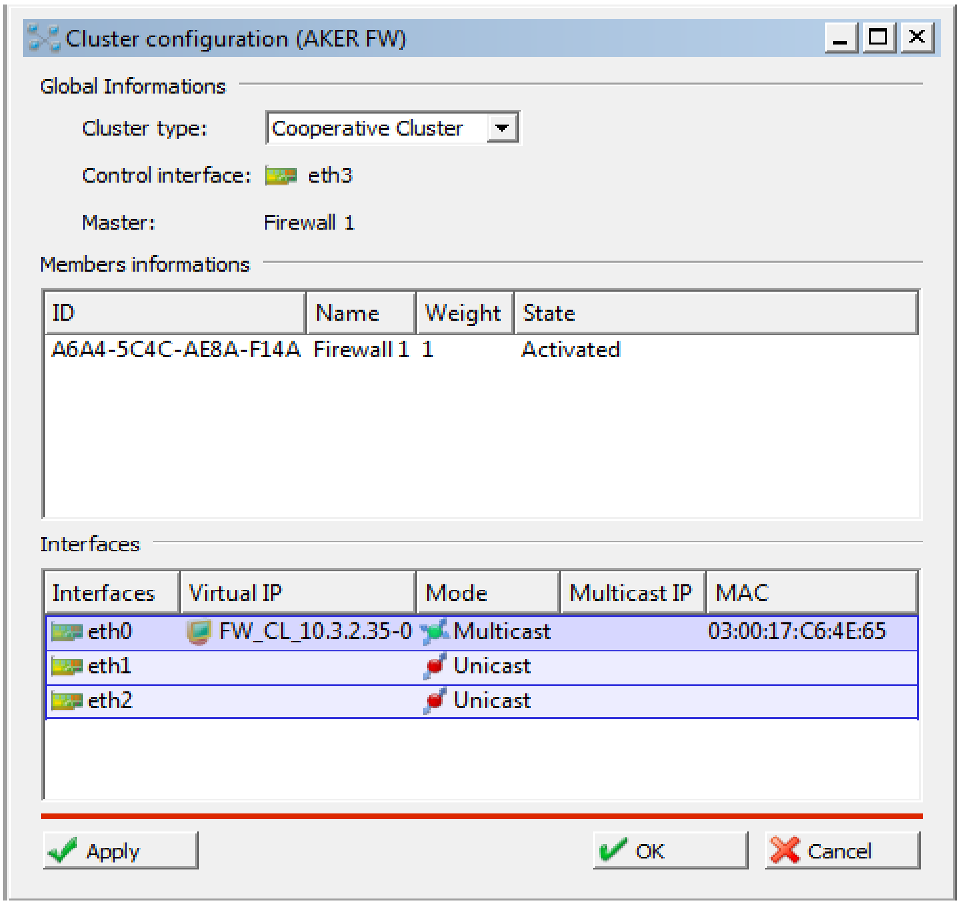
ID	Name	Weight	State
A6A4-5C4C-AE8A-F14A	Firewall 1	1	Activated

Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0	FW_CL_10.3.2.35-0	Multicast		03:00:17:C6:4E:65
eth1		Unicast		
eth2		Unicast		

Image 573 – Registering MAC

After the procedure above the Cooperative cluster will be created.



Global Informations

Cluster type: Cooperative Cluster

Control interface: eth3

Master: Firewall 1

Members informations

ID	Name	Weight	State
A6A4-5C4C-AE8A-F14A	Firewall 1	1	Activated

Interfaces

Interfaces	Virtual IP	Mode	Multicast IP	MAC
eth0	FW_CL_10.3.2.35-0	Multicast		03:00:17:C6:4E:65
eth1		Unicast		
eth2		Unicast		

Image 574 – Created cooperative cluster

37.5. Using the Text Interface

This interface has the same capability as the Remote Interface and it is very simple to be used.

Program location: /aker/bin/firewall # fwcluster
/aker/bin/firewall # fwcluster

```
Aker Firewall
Usage: fwcluster [help | show]
    fwcluster type <off | failover | ha | coop>
    fwcluster interface_control <if>
    fwcluster weight <weight>
    fwcluster name <name>
    fwcluster <enable | disable> [master / slave] [ -f ]
    fwcluster <add | delete> <if> [host | -f]
    fwcluster <mode> <if> [multicast [igmp <ip>] [mac <mac>] | unicast]
    fwcluster clear [ -f ]
(!) where:
    if      : Interface entity name
    weight    : this firewall weight in the cluster
    host : virtual IP address to be include or removed (host entity)
    master  : optional argument that will indicate this host as master
    slave   : optional argument that will indicate this host as slave
    -f      : optional argument that forces the configuration implementation
even with the Control Center authenticated.
```

Exemplo 1: (showing the configuration)

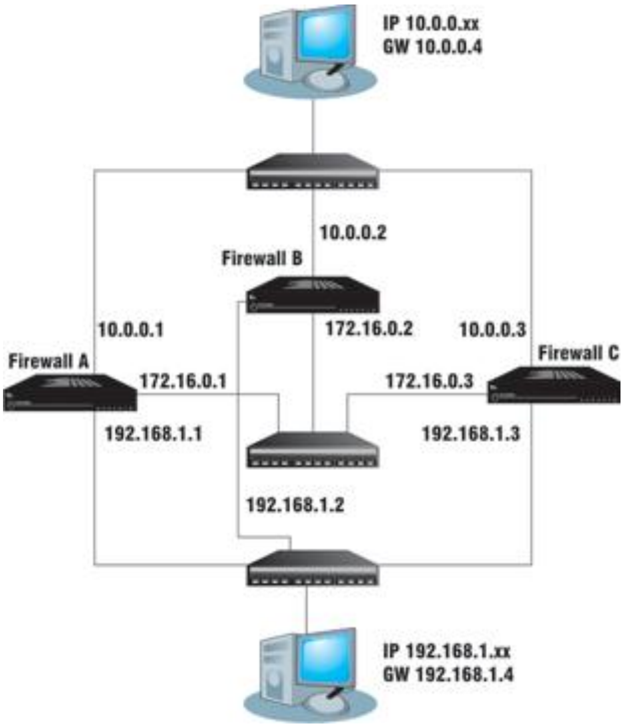

IP 10.0.0.xx
GW 10.0.0.4
10.0.0.2
Firewall B
10.0.0.1
172.16.0.2
10.0.0.3
Firewall A
Firewall C
172.16.0.1
172.16.0.3
192.168.1.1
192.168.1.3
192.168.1.2
IP 192.168.1.xx
GW 192.168.1.4

Image 575 – Showing the interface configuration.

Before begin to create a cluster, you have to register all interfaces, remembering that all firewalls have different IP addresses.

Examples: Firewall A – rl0 – if_external – 10.0.0.1 Firewall B – rl0 – if_external – 10.0.0.2
rl1 – if_internal – 192.168.1.1 rl1 – if_internal – 192.168.1.2
rl2 – if_control – 172.16.0.1 rl2 – if_control – 172.16.0.2

Firewall C – rl0 – if_external – 10.0.0.3
rl1 – if_internal – 192.168.1.3
rl2 – if_control – 172.16.0.3

Following create a virtual entity for each one of the network adapters, except for the Control Interface. These entities shall have the same value to all firewalls used in the cluster.

Examples: Firewall A – external_firewall (ip 10.0.0.4) Firewall B – external_firewall (ip 10.0.0.4)
internal_firewall (ip 192.168.1.4) internal_firewall (ip 192.168.1.4)

Firewall C – external_firewall (ip 10.0.0.4)
internal_firewall (ip 192.168.1.4)

Cluster hosts do not need to be equal, but the network adapters need to.

To use the failover cluster uses only 2 firewalls, since only one will respond all traffic.

System Files

38. System files

This chapter shows where are and what are the System Files used for.

38.1. System files

In this topic, the systems files and their location will be displayed. This is very important for backups and troubleshooting

Directory Tree

- **/etc/firewall** – contains executable programs and sub-directories
- **/etc/firewall/x509** – X.509 certificate files
- **/etc/firewall/httpd** – root of the file system of the local HTTP server of the WWW proxy. Do not remove the files already present in this directory.
- **/etc/firewall/conf** – firewall configuration files
- **/etc/firewall/snmpd** – has the SNMP agent
- **/var/log** – log and event files of Aker Firewall
- **/var/spool/firewall** – used by the SMTP and POP3 proxies to store messages to be sent.

Executable Programs

Programs that can be executed by Aker Firewall administrator

- **/etc/firewall/fwadmin** – Command line interface for the user administration
- **/etc/firewall/fwaction** – Command line interface for the system's actions configuration
    - **/aker/bin/firewall/fwblink –** Command line interface for the link load balancing configuration.
    - **/aker/bin/firewall/fwkey –** Command line interface for the system's activation key configuration
- **/etc/firewall/fwclient** – Command line interface for the encryption clients access configuration
- **/etc/firewall/fwcluster** – Command line interface for the fault tolerance configuration
- **/etc/firewall/fwcripto** – Command line interface for the encryption and authentication configuration
    - **/aker/bin/firewall/fwedpwd –** Command line interface to configure the local authentication database
    - **/aker/bin/firewall/fwent –** Text Interface command used in the entities creation.
    - **/aker/bin/firewall/fwflood –** Text Interface command used to configure the protection against SYN flood.

- **/aker/bin/firewall/fwids –** Command line interface used to configure the External IDS agents.
- **/aker/bin/firewall/fwaccess –** Command line interface used to configure the access profiles associations.
- **/aker/bin/firewall/fwlist –** Command line interface used to access the connections and sessions of active users.
- **/aker/bin/firewall/fwlog –** Command line interface used to access the firewall logs and events.
- **/aker/bin/firewall/fwmaxconn –** Command line interface used to configure the Flood protection.
- **/aker/bin/firewall/fwnat –** Command line interface used to configure the address translation (NAT) configuration
- **/aker/bin/firewall/fwpar –** Command line interface used to configure the global parameters
- **/aker/bin/firewall/fwrule –** Command line interface used to *configure the stateful inspection rules table*.
- **/aker/bin/firewall/fwipseccert –** Command line interface used to manage the x.509 certificates required for IPSEC encryption.
- **/aker/bin/firewall/fwstat –** Command line interface to configure and view the firewall statistics.
- **/aker/bin/common/akinterface –** Command line interface for firewall network interface configuration.
- **/aker/bin/firewall/fwauth –** Command line interface the global parameters of the firewall authentication.
- **/aker/bin/firewall/akddns** – Command line interface for the DDNS client configuration.
- **/aker/bin/firewall/fwadvroute** – Command line interface for the advanced routing configuration.
- **/aker/bin/firewall/fwedpwd –** Command line interface used to configure firewall local authenticator users.
- **/aker/bin/firewall/akhwsig** – shows the hardware signature.
- **/aker/bin/firewall/fwl2tp** – Command line interface for the L2TP VPN configuration;
- **/aker/bin/firewall/fwpptpsrv –** Text Interface command for the PPTP VPN configuration;
- **/aker/bin/firewall/fwlic** – shows the information about the use of limited license for ip.
- **/aker/bin/firewall/fwpacket** – Command line interface for Aker firewall dumps collection.
- **/aker/bin/firewall/fwportscan** – Command line interface for the *PORTSCAN* detection filter configuration.
- **/aker/bin/firewall/fwver** – show the version and the build date of the Firewall files.

Programs that should not be executed directly by the administrator

- **/aker/bin/firewall/2.6.x/aker_firewall_mod-xxxx.o** – Loadable Kernel module with the firewall (Linux only).
- **/aker/bin/firewall/fwauthd** – Users' authentication server
- **/aker/bin/firewall/fwcardd** – X.509 certificates validation module for smart cards

- **/aker/bin/firewall/fwconfd** – Communication server for the Remote Interface
- **/aker/bin/firewall/fwcrld** – CRLs download module of active certificate authority
- **/aker/bin/firewall/fwcryptd** – Encryption server for clients
- **/aker/bin/firewall/fwdnsd** – DNS name resolution server for the Remote Interface.
- **/aker/bin/firewall/fwidsd –** Program used in the communication with the intrusion detection agent.
- **/aker/bin/firewall/fwinit –** Aker Firewall startup program
- **/aker/bin/firewall/fwftppd –** FTP transparent proxy
- **/aker/bin/firewall/fwgkeyd** – Encryption key generation server
- **/aker/bin/firewall/fwhttppd** – HTTP transparent proxy and non-transparent web filter
- **/aker/bin/firewall/fwheartd** – Cluster control service
- **/aker/bin/firewall/fwhconfd** – Cluster distributed configuration service
- **/aker/bin/firewall/fwgenericstd** – Cluster information collection service
- **/aker/bin/firewall/fwstconnd** – Cluster connections replication service
- **/aker/bin/firewall/fwlinkmond** – Links monitoring service
- **/aker/bin/firewall/fwdlavd** – Web antivirus service
- **/aker/bin/firewall/fwmachined** – Performance information collection service
- **/aker/bin/firewall/fwpmapd** – RPC transparent proxy
- **/aker/bin/firewall/fwlkeyd** – Encryption certificate server
- **/aker/bin/firewall/fwmond** – Monitoring module and restart of firewall process
- **/aker/bin/firewall/fwnatmond** – Monitoring module of hosts for the load balancing
- **/aker/bin/firewall/fwprofd** – Users' login server
- **/aker/bin/firewall/fwrapd –** Real Player transparent proxy
- **/aker/bin/firewall/fwrtspd –** Real Time Streaming Protocol
- **/aker/bin/firewall/fwsocksd –** SOCKS non-transparent proxies
- **/aker/bin/firewall/fwsmtppd –** SMTP transparent proxy
- **/aker/bin/firewall/fwpop3pd –** POP3 transparent proxy
- **/aker/bin/firewall/fwlogd –** Log, events and statistics server
- **/aker/bin/firewall/fwscanlogd –** Log, events and statistics research server
- **/aker/bin/firewall/fwsyncd** – Sync and encryption seed generation process
- **/aker/bin/firewall/fwtelnetd –** Telnet transparent proxy
- **/aker/bin/firewall/fwtrap** – Module of sending SNMP traps
- **/aker/bin/firewall/fwurld** – Testing and analysis module of URLs access permission
- **/aker/bin/firewall/fwiked** – key trading module for IPSEC encryption (IKE protocol)
- **/aker/bin/firewall/fwtunneld –** Secure Roaming Server for Firewall
- **/aker/bin/firewall/libaker.so** – Generic Firewall Library
- **/aker/bin/firewall/libconfd.so** – Firewall Library configuration
- **/aker/bin/firewall/snmpd/snmpd** – SNMP agent
- **/aker/bin/firewall/corr.fw** – Contains the correction level applied
- **/aker/bin/firewall/fwadmkeys** – RSA key generator
- **/aker/bin/firewall/fwapply** – Assists applying patches
- **/aker/bin/firewall/fwarpd** – ARP request response
- **/aker/bin/firewall/fwdcerpcd** – Proxy DCE-RPC.
- **/aker/bin/firewall/fwdeepd –** IPS/IDS module and application filtering;
- **/aker/bin/firewall/fwh2250pd –** H.323. proxy

- **/aker/bin/firewall/fwh245pd –** H.323 proxy.
- **/aker/bin/firewall/fwhwid –** Process that creates a unique host identifier.
- **/aker/bin/firewall/fwmsnd –** MSN proxy.
- **/aker/bin/firewall/fwpptpd** – Module that allows PPTP connection pass through the address translation (NAT)
- **/aker/bin/firewall/fwpptpradiusd** – VPN LPPTP authentication module
- **/aker/bin/firewall/fwpscand** – PORTSCAN detection module
- **/aker/bin/firewall/fwquotad** – Quota control module.
- **/aker/bin/firewall/fwreportd** – Report generator module.
- **/aker/bin/firewall/fwrollback** – Assists on the patches rollback.
- **/aker/bin/firewall/fwsipd** – SIP Proxy
- **/aker/bin/firewall/fwsslpd** – VPN SSL and SSL proxy module.
- **/aker/bin/firewall/fwtraind** – Aker Spam Meter emails training module.
- **/aker/bin/firewall/fwtunneldpt.qm** – Translation files
- **/aker/bin/firewall/fwupdatepatchhis** – Assists patches management.
- **/aker/bin/firewall/fwzebrad** – OSPF and RIP advanced routing module.
- **/aker/bin/firewall/fwvlan** – VLAN 802.1q creation module
- **/aker/bin/firewall/hostapd_run.sh –** Runs the HOSTAPD command.
- **/aker/bin/firewall/l2tpns** – VPN L2TP module;
- **/aker/bin/firewall/libh323.so.1.0.0** – Support library for the H.323 proxy
- **/aker/bin/firewall/nsctl –** Assists l2tpns
- **/aker/bin/firewall/rc.aker** – Firewall default launcher
- **/aker/bin/firewall/rpt_files** – Report files
- **/aker/bin/firewall/squid** – Cache files
- **/aker/bin/firewall/strings** – Assists the FWVER.

Stats, Events and Log Files

- **/var/log/fw-650-AAAAMMDD.fwlg –** Stores firewall logs of date YYYY/MM/DD
- **/var/log/fw-650-AAAAMMDD.fwev –** Stores firewall events of date YYYY/MM/DD
- **/var/log/stat-650-AAAAMMDD.fws –** Stores firewall stats of date YYYY/MM/DD

Aker Firewall BOX

39. Aker Firewall Box

This chapter shows the commands that can be used on Aker Firewall box shell.

Aker Firewall Box

Aker Firewall Box is an appliance, that is, an integrated solution of hardware and software. The great advantage of this platform is that it does not require any knowledge of any operating system. Besides, by having its entire configuration stored in a flash memory and because it is an industrial hardware, the platform presents more resistance against problems, especially those caused by energy problems.

Aker Firewall Box is available on several different models that are designed to fulfill the needs of small, medium and large companies.

The complete list of all available models is frequently updated and can be viewed at:

http://www.aker.com.br

How does Aker Firewall box shell work?

When a remote terminal configured at 9600 bps is connected to the corresponding serial interface on an Aker Firewall Box, it is possible to use its shell.

When this procedure is performed, it is first necessary to press the Enter key, until the password prompt appears. The initial password is '123456' and if it is type correctly, the following prompt will be displayed:

```
Aker>
```

In case the local access password of the firewall is lost, it is necessary to contact the technical support in order to initiate the password reset procedure.

In the shell prompt, all standard commands of Aker Firewall can be typed, as described on the topics covering the command line interface on each chapter. In addition of those, there are specific commands of Aker Firewall box that are documented below:

It is possible to type the firewall commands in the shell without the fw prefix, that is, "**ent**" instead of fwent (to use the commands without the "FW" prefix the user needs enter the command "akshell" before using the command with "FW" prefix)

To exit from the shell, it is enough to type in the commands exit or quit or simply to press the Ctrl + D keys.

Specific commands of Aker Firewall Box

Command	quit exit
Description	Finish the shell session

Command	help ?
Description	Show a list with all valid commands

Command	shutdown
Description	Shuts down the firewall, so it can be turned off

Command	reboot
Description	Reboots the firewall

Command	ping [-c n_pkt] [-i interv] ip_destination
Description	Sends ping packets and waits for replies The -c option specifies the number of packets to be sent The -i option specifies the transmission interval between the packets in milliseconds (ms)

Command	password
Description	Changes the firewall local access password

Command	date <show> | <dd/mm/aaaa>
Description	With the show argument informs the system date. Otherwise sets the date to the informed value.

Command	time <show> | <hh:mm[:ss]>
Description	With the show argument informs the system time. Otherwise sets the time to the informed value.

AWCA Plugin manual - Aker Web Content Analyzer

40. Aker Web Content Analyzer – AWCA

This chapter shows how to use AWCA on Aker Firewall.

40.1. Introduction

The internet is an essential tool in the corporate environment. However if misused it can compromise the productivity of employees. Having this in mind, several organizations began to adopt use policies, imposing some access restrictions.

To meet this new demand, **Aker Security Solutions** developed **Aker Web Content Analyzer**. The product offers a broad base of URL, with daily update made by qualified professionals.

Aker Web Content Analyzer is a safe and smart tool, which is focused on provide the clients solutions for monitoring and real-time control of Internet usage of your company's employees, grating or blocking access to specifics websites, setting a specific time to users use the Internet (e.g. from 12:00 p.m. until 2 p.m. users are allowed to access the Internet, after 2 p.m. the access will be denied.), antivirus protection and reports describing what has been used by users or groups.

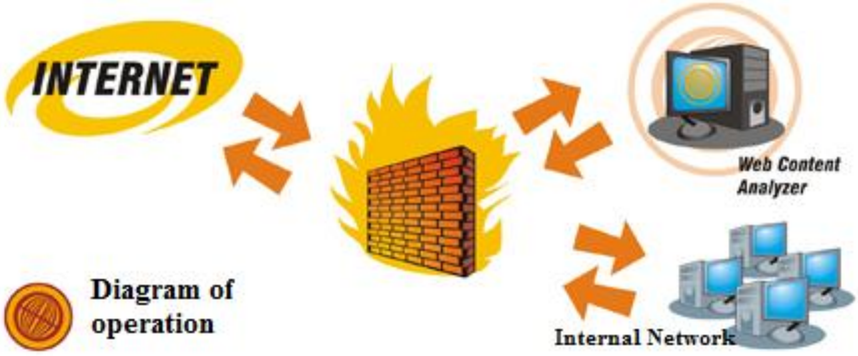


Image 576 – Web Content Analyzer diagram of operation.

For each connection request, the system identifies the website classification on the URL analyzer's database and determines if the user will be able to access the website or not, based on the user's profile. As the Analyzer works together with the

Identifier, **Aker Firewall access profiles** can set single profiles specifying the type of content that each user will have access to.

This tool also works with **Aker Web Control** that has configuration plugins for Microsoft ISA Server®, SQUID Server® and for Firewall Checkpoint®.

Aker Web Control for Squid is a program that allows Squid to accept or reject access according to the access level of each user and the desired page category.

Aker Web Control for ISA Server is a program that allows ISA Server to accept or rejects access according to the access level of each user and desired page category.

All of these features are part of **Web Content Analyzer** which is a powerful tool for Internet access control.

40.2. Prerequisite

Software

Aker Web Content Analyzer runs on the following operating system: Windows and Linus GNU platforms Intel 32 bits or compatible.

It is compatible to Aker Firewall, MS Proxy Server and MS ISA Server, Checkpoint Firewall 1 and Squid Internet Object Cache. Except Aker Firewall, the other products need a plugin to communicate with **Aker Web Content Analyzer.**

Hardware

The hardware requirements many vary according to the amount of simultaneous clients and their links. The minimum requirement is:

- Pentium 1 Ghz or higher;
- 256 Mbytes RAM;
- Hard Drive 2 GB of free space;
- Monitor;
- Ethernet card.

Before using this program user shall verify if all requirements are supported by the operating system in use.

40.3. Installing Aker Web Content Analyzer

O Aker Web Content Analyzer runs on the following versions of operating system:

- Windows Server: 2000, 2003 e 2008;
- Linux GNU;

The following screens will show how Aker Web Content Analyzer is installed:

40.4. Installation on a windows platform

Download the installer at http://www.aker.com.br

Select a language (English or Portuguese), then click on **"OK"**.

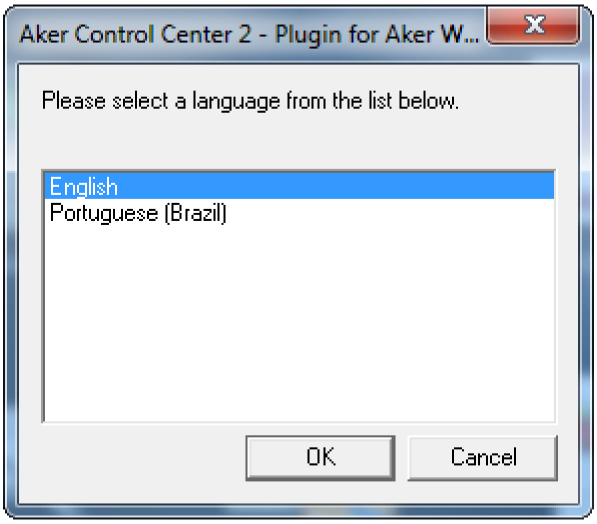
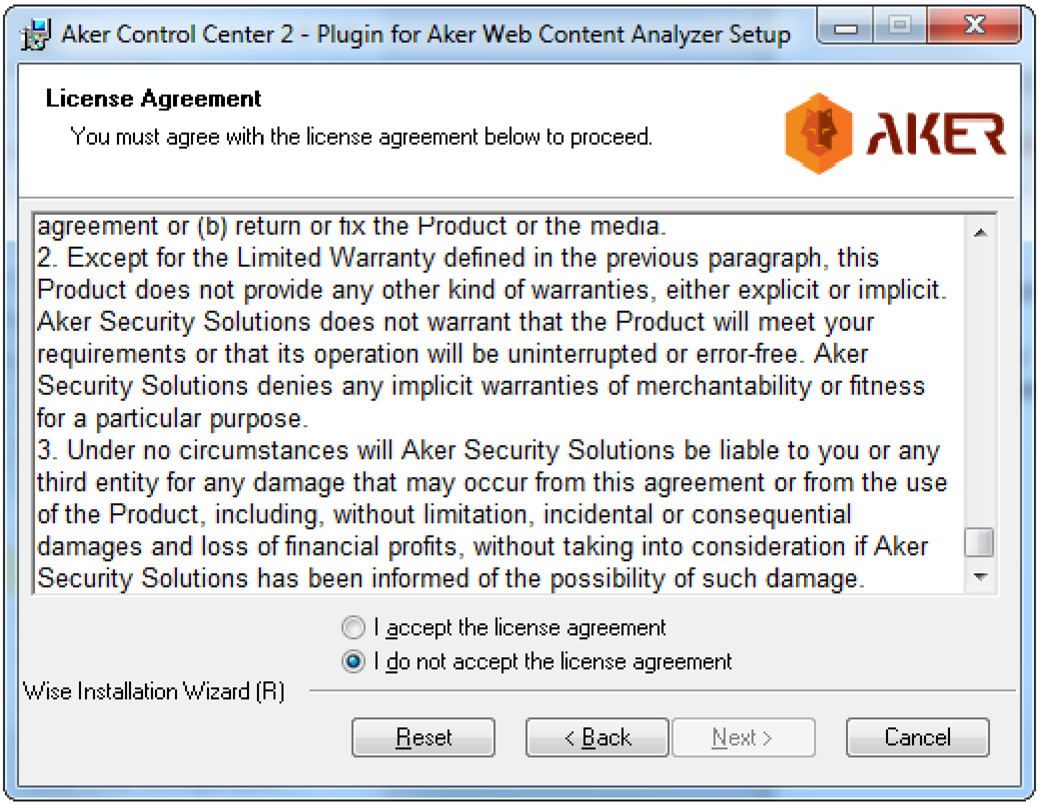

Aker Control Center 2 - Plugin for Aker W...
Please select a language from the list below.
English
Portuguese (Brazil)
OK
Cancel

Image 577 – Select the language you wish to continue the installation.

License Agreement

Read the License Agreement in case you agreed select the option **"I accept the license agreement".** Then click on **"Next".**



Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup

License Agreement

You must agree with the license agreement below to proceed.

agreement or (b) return or fix the Product or the media.
2. Except for the Limited Warranty defined in the previous paragraph, this Product does not provide any other kind of warranties, either explicit or implicit. Aker Security Solutions does not warrant that the Product will meet your requirements or that its operation will be uninterrupted or error-free. Aker Security Solutions denies any implicit warranties of merchantability or fitness for a particular purpose.
3. Under no circumstances will Aker Security Solutions be liable to you or any third entity for any damage that may occur from this agreement or from the use of the Product, including, without limitation, incidental or consequential damages and loss of financial profits, without taking into consideration if Aker Security Solutions has been informed of the possibility of such damage.

○ I accept the license agreement
● I do not accept the license agreement

Image 578 – License Agreement.

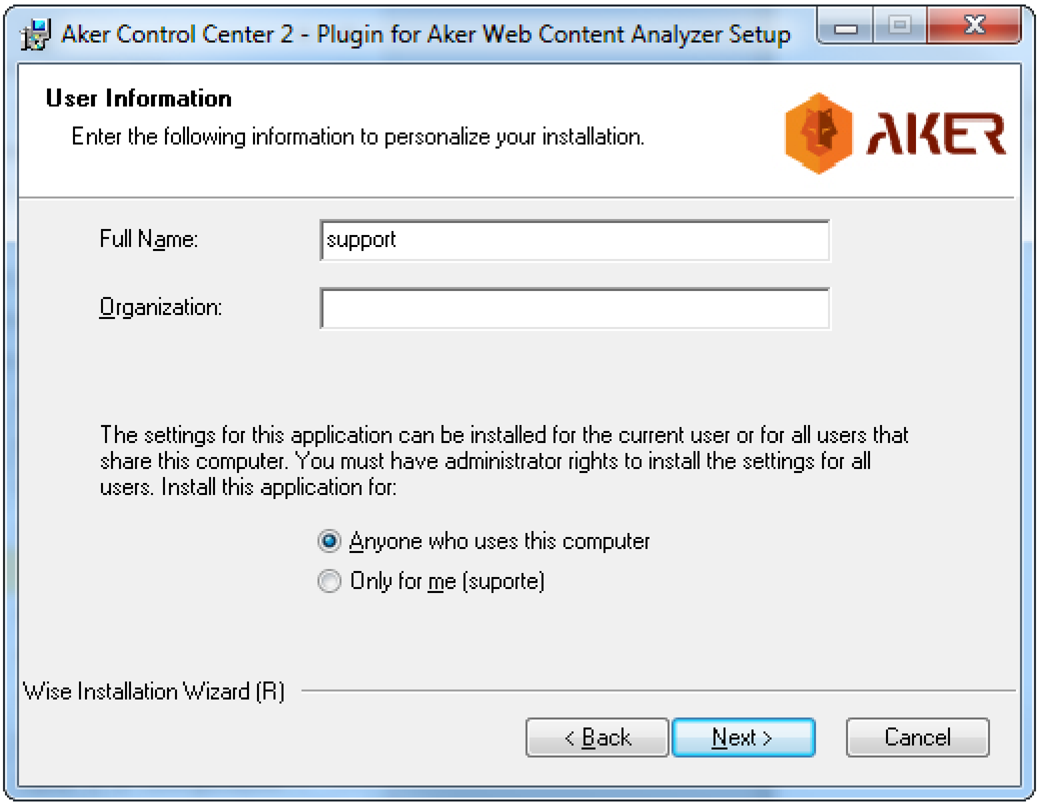
User Information

Type the user’s **“Full Name**”.

Type the **“Company’s”** name.

Select if the application will be installed for **“Anyone who uses this computer”** or the option **“Only for me”**

Click on **“Next”**


Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup
AKER
< Back
Next >
Cancel

User Information

Enter the following information to personalize your installation.

Full Name: support

Organization:

The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:

● Anyone who uses this computer

○ Only for me (suporte)

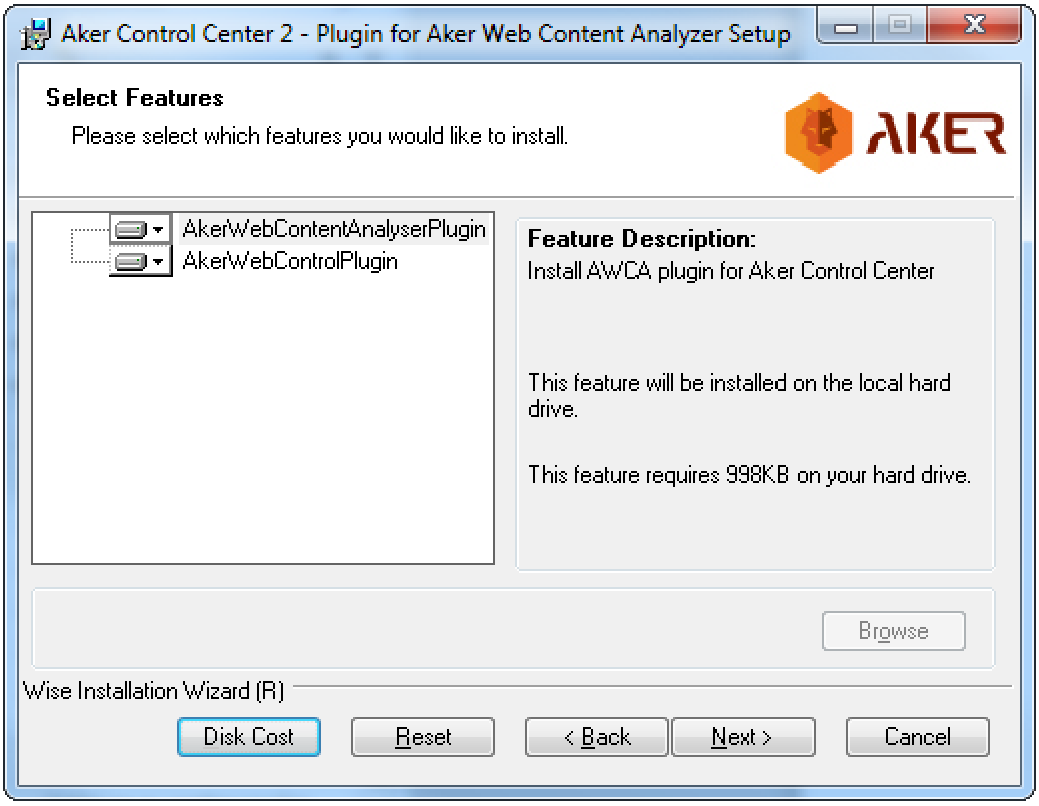
Wise Installation Wizard (R)

Image 579 – User Information

Features selection

Choose **"AkerWebContentAnalyzerPlugin"** then click on **"Next"**.

Aker Web Content Analyzer installation plugin comes together with Aker **Web Control** plugin, i.e. it will be automatically installed. In case you do not wish to install **Aker Web Control Plugin**, select the option **"Entire feature will be unavailable"**



Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup

Select Features

Please select which features you would like to install.

AkerWebContentAnalyserPlugin
AkerWebControlPlugin

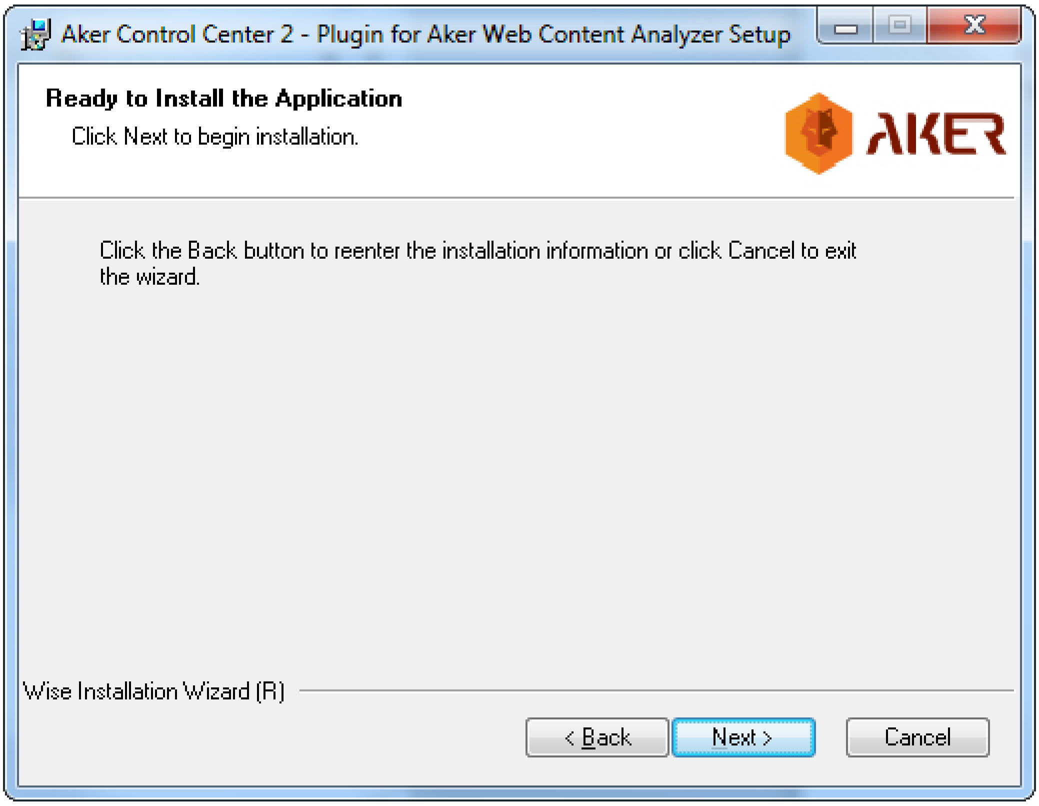
Feature Description:
Install AWCA plugin for Aker Control Center

This feature will be installed on the local hard drive.

This feature requires 998KB on your hard drive.

Image 580 – Features selection

Following the message **“Ready to Install the Application**” will be displayed. Click on **“Next”** to begin the installation.



Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup

Ready to Install the Application

Click Next to begin installation.

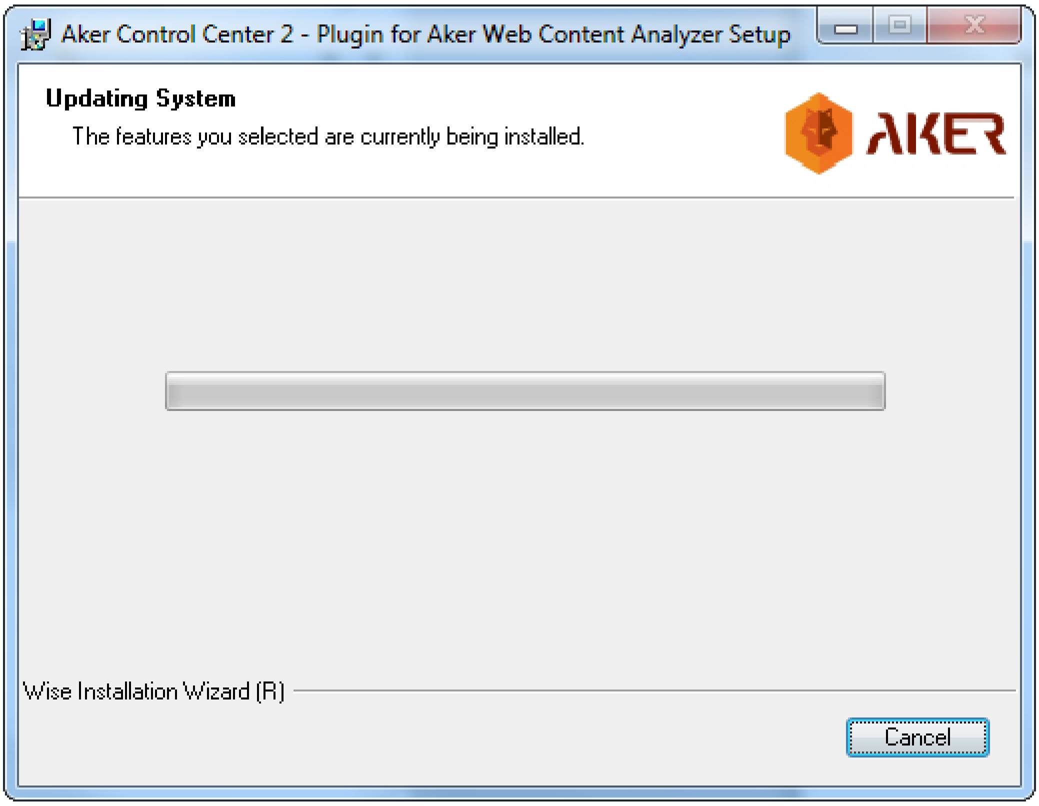
Click the Back button to reenter the installation information or click Cancel to exit the wizard.

Wise Installation Wizard (R)

Image 581 – Ready to install message

Updating System

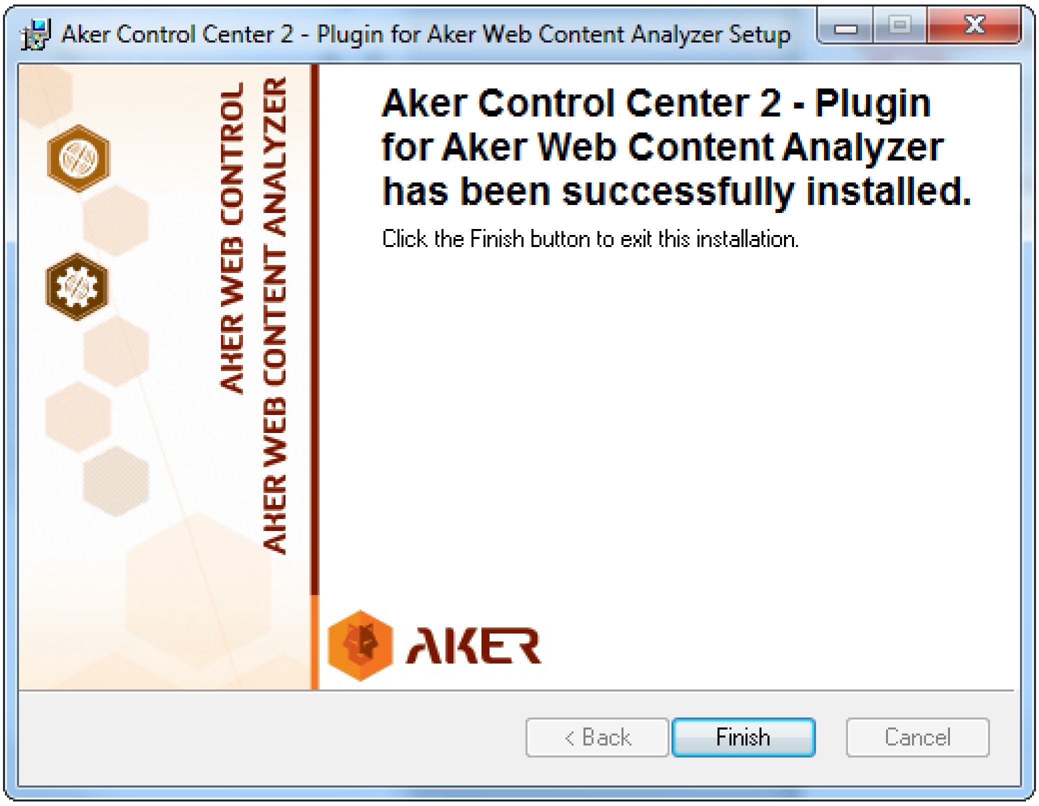
The updating System window will show the installation progress bar.



Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup
Updating System
The features you selected are currently being installed.
AKER
Wise Installation Wizard (R)
Cancel

Image 582 – Installation progress bar.

When the installation is completed the message **"Aker Control Center 2 – Plugin for Aker Web Content Analyzer has been successfully installed"** will be displayed. Now simply click on **"Finish".**



Aker Control Center 2 - Plugin for Aker Web Content Analyzer Setup

Aker Control Center 2 - Plugin for Aker Web Content Analyzer has been successfully installed.

Click the Finish button to exit this installation.

AKER WEB CONTROL
AKER WEB CONTENT ANALYZER
AKER
< Back
Finish
Cancel

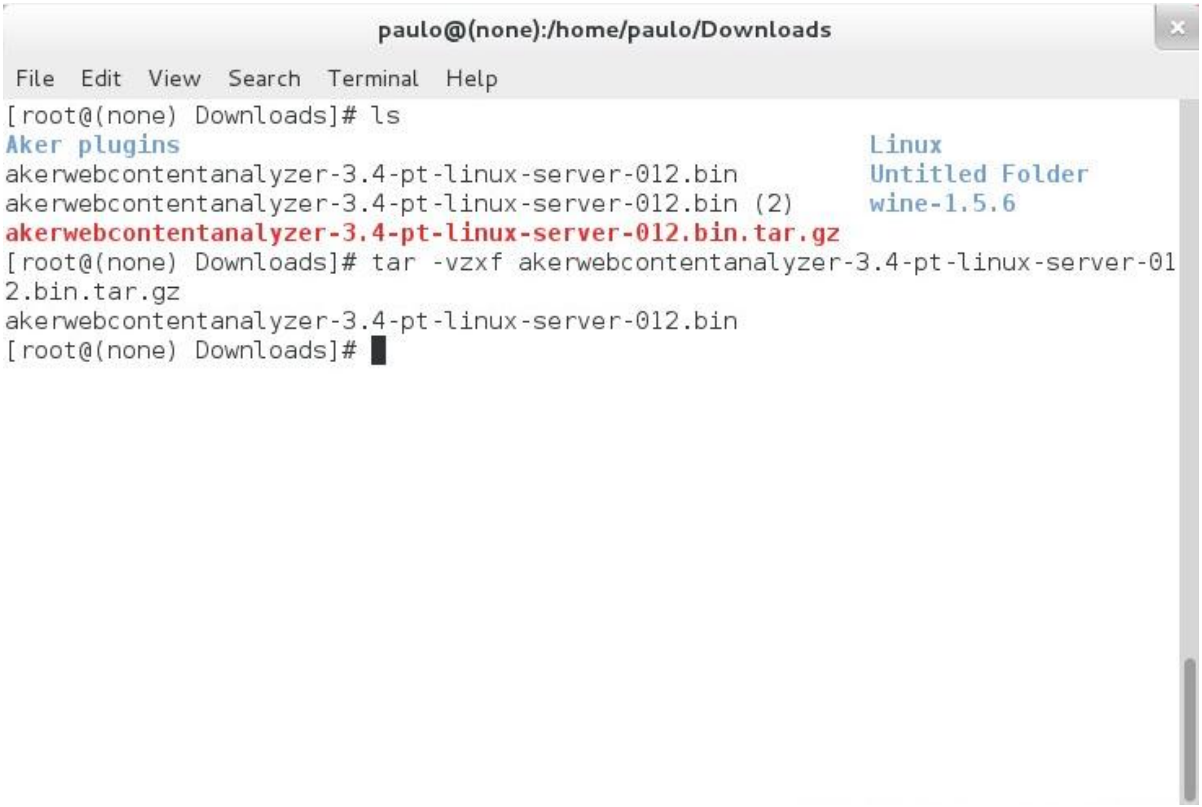
Image 583 – Installation has been completed

40.5. Installation on a Linux platform (Fedora)

The installation on Linux platform is very simple: create a directory and copy the file **AkerWebContentAnalyzer-server-br-3.0-3.fc8.tar.bz2**.

In case your file is zipped use the following command:

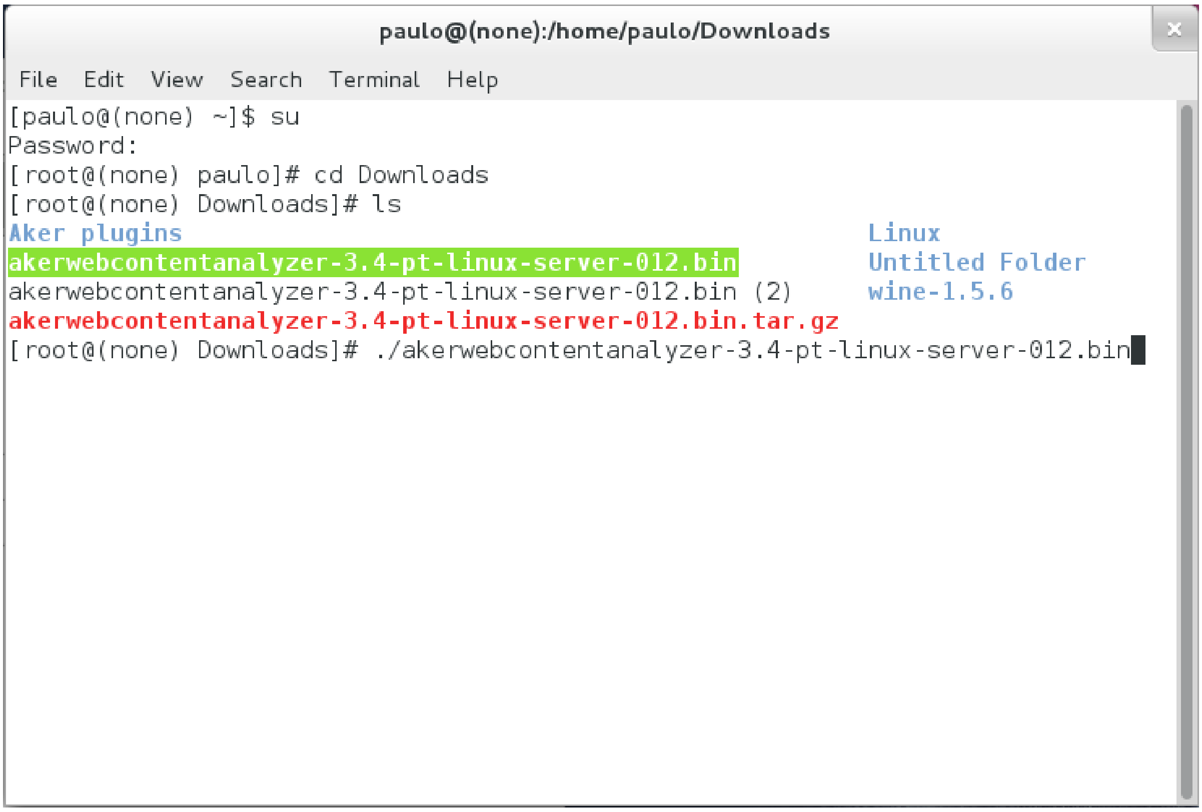
tar -vzxf akerwebcontentanalyzer-3.4-pt-linux-server-012.bin.tar.gz


paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
[root@(none) Downloads]# ls
Aker plugins                                               Linux
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin         Untitled Folder
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin (2)     wine-1.5.6
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin.tar.gz
[root@(none) Downloads]# tar -vzxf akerwebcontentanalyzer-3.4-pt-linux-server-01
2.bin.tar.gz
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin
[root@(none) Downloads]# 
```

Image 584 – Linux Installation: Unzipping.

Access the directory you have copied the file to and use the following command: **./akerwebcontentanalyzer-3.4-pt-linux-server-012.bin**

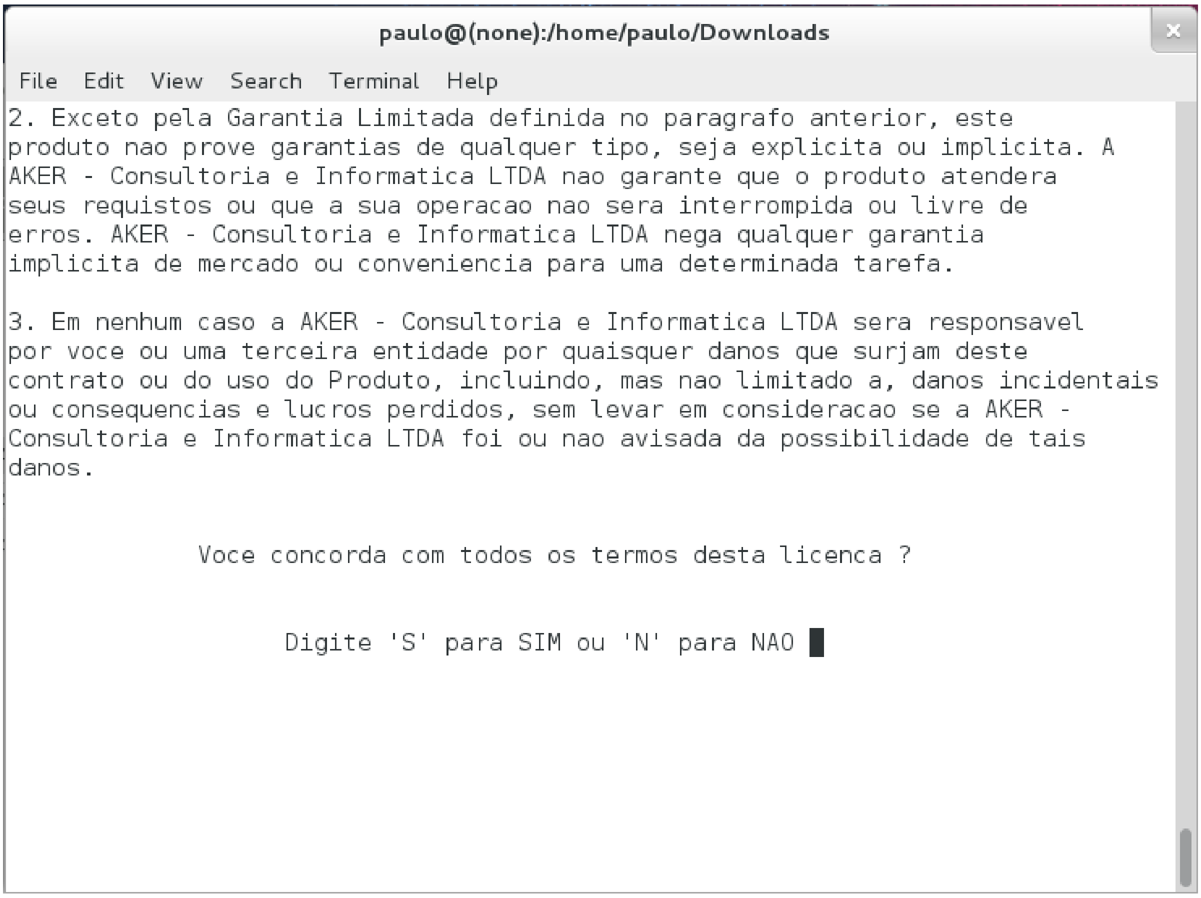

paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
[paulo@(none) ~]$ su
Password:
[root@(none) paulo]# cd Downloads
[root@(none) Downloads]# ls
Aker plugins                                                 Linux
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin          Untitled Folder
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin (2)      wine-1.5.6
akerwebcontentanalyzer-3.4-pt-linux-server-012.bin.tar.gz
[root@(none) Downloads]# ./akerwebcontentanalyzer-3.4-pt-linux-server-012.bin
```

Image 585 – Linux Installation: Installing AWCA.

The system will show the license agreement.

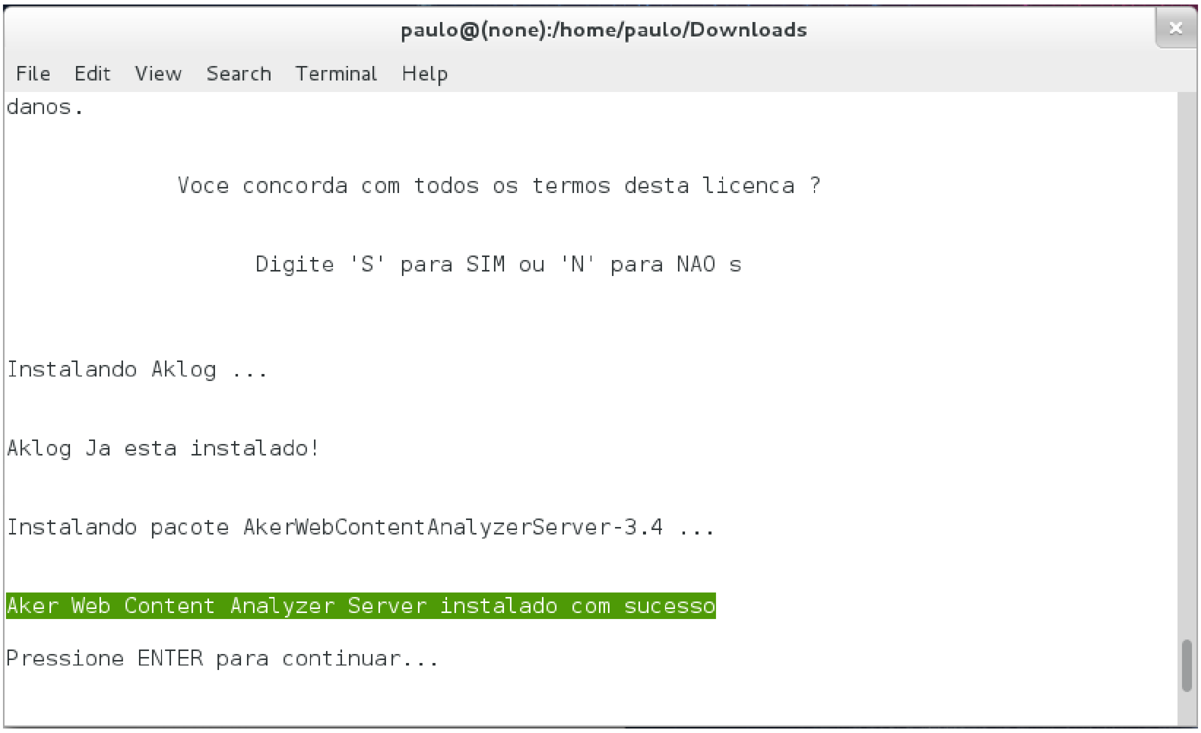
Type **“Y” (yes)** to agree or **“N” (no)** to disagree and abort the installation.


paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
2. Exceto pela Garantia Limitada definida no paragrafo anterior, este
produto nao prove garantias de qualquer tipo, seja explicita ou implicita. A
AKER - Consultoria e Informatica LTDA nao garante que o produto atendera
seus requistos ou que a sua operacao nao sera interrompida ou livre de
erros. AKER - Consultoria e Informatica LTDA nega qualquer garantia
implicita de mercado ou conveniencia para uma determinada tarefa.

3. Em nenhum caso a AKER - Consultoria e Informatica LTDA sera responsavel
por voce ou uma terceira entidade por quaisquer danos que surjam deste
contrato ou do uso do Produto, incluindo, mas nao limitado a, danos incidentais
ou consequencias e lucros perdidos, sem levar em consideracao se a AKER -
Consultoria e Informatica LTDA foi ou nao avisada da possibilidade de tais
danos.


             Voce concorda com todos os termos desta licenca ?


                   Digite 'S' para SIM ou 'N' para NAO
```

Image 586 – License agreement

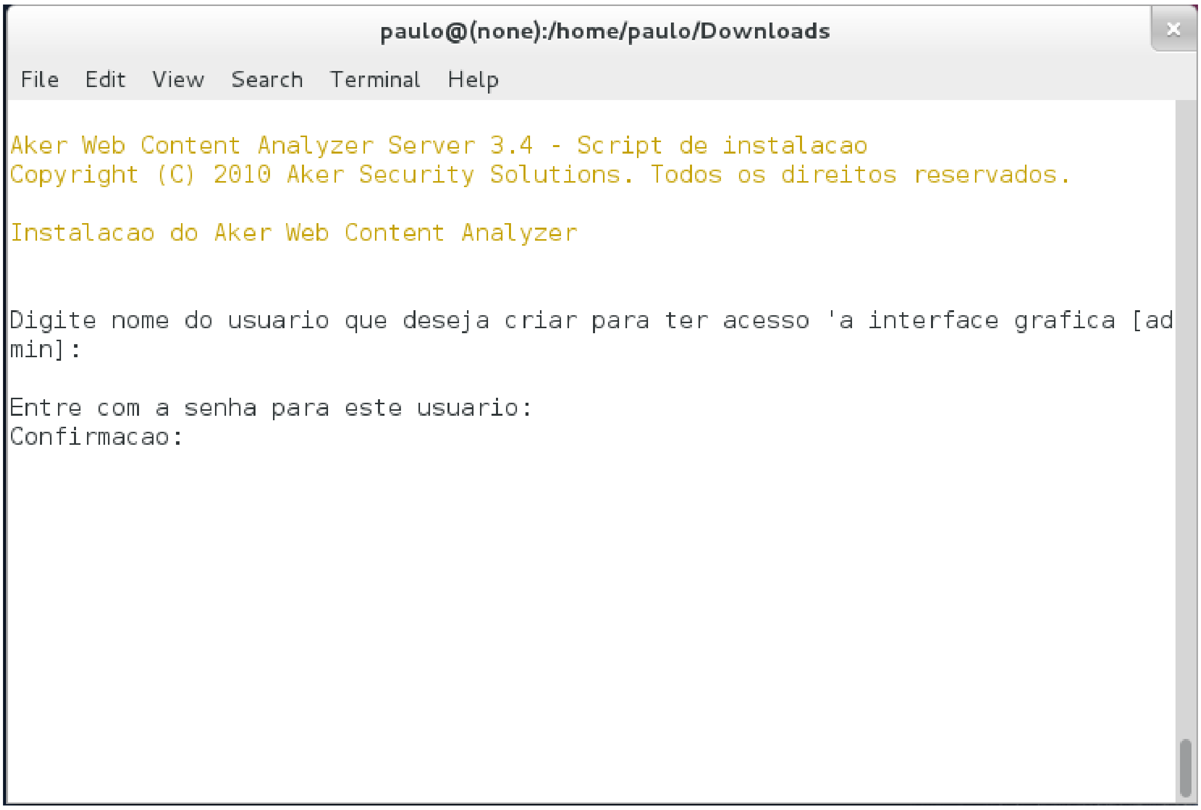
Now the installation script will verify if there is a product log module (AKLOGD), and install one in case no module log is detected.


paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
danos.


             Voce concorda com todos os termos desta licenca ?


                   Digite 'S' para SIM ou 'N' para NAO s



Instalando Aklog ...


Aklog Ja esta instalado!


Instalando pacote AkerWebContentAnalyzerServer-3.4 ...


Aker Web Content Analyzer Server instalado com sucesso

Pressione ENTER para continuar...
```

Image 588 – Installing AKLOGD (log module)

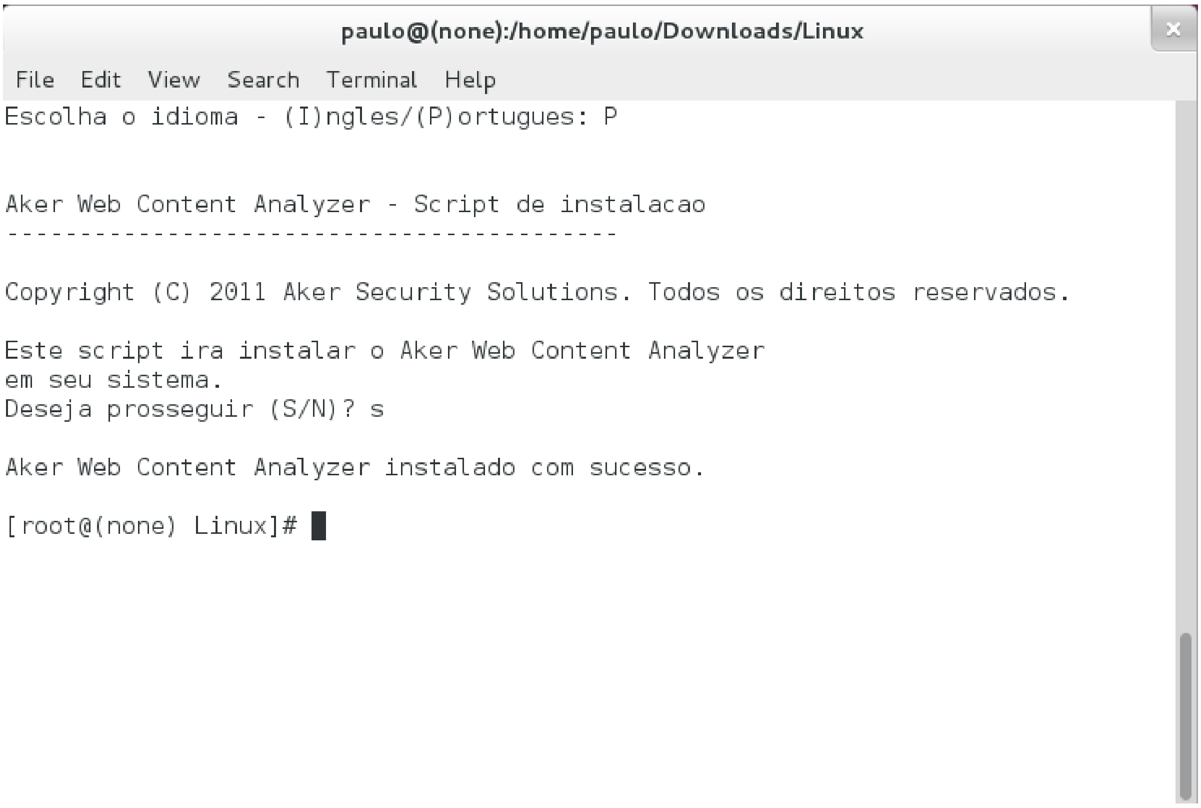
Next step you will create user to administrate the Remote Interface. You can neither choose a user name, or simply hit **“Enter”** and a user named (admin) will be created. After type the password.


paulo@(none):/home/paulo/Downloads
File Edit View Search Terminal Help

```
Aker Web Content Analyzer Server 3.4 - Script de instalacao
Copyright (C) 2010 Aker Security Solutions. Todos os direitos reservados.

Instalacao do Aker Web Content Analyzer


Digite nome do usuario que deseja criar para ter acesso 'a interface grafica [ad
min]:

Entre com a senha para este usuario:
Confirmacao:
```

Image 589 – Setting user name and password.

Press **“enter”** in order to complete the installation.


paulo@(none):/home/paulo/Downloads/Linux
File Edit View Search Terminal Help

```
Escolha o idioma - (I)ngles/(P)ortugues: P


Aker Web Content Analyzer - Script de instalacao
------------------------------------------

Copyright (C) 2011 Aker Security Solutions. Todos os direitos reservados.

Este script ira instalar o Aker Web Content Analyzer
em seu sistema.
Deseja prosseguir (S/N)? s

Aker Web Content Analyzer instalado com sucesso.

[root@(none) Linux]# 
```

Image 590 – Linux Installation: Creating a user administrator.

40.6. AWCA configuration

To gain access to the AWCA configuration window, select the **Remote device**, and click on the **Web Content Analyzer** menu.

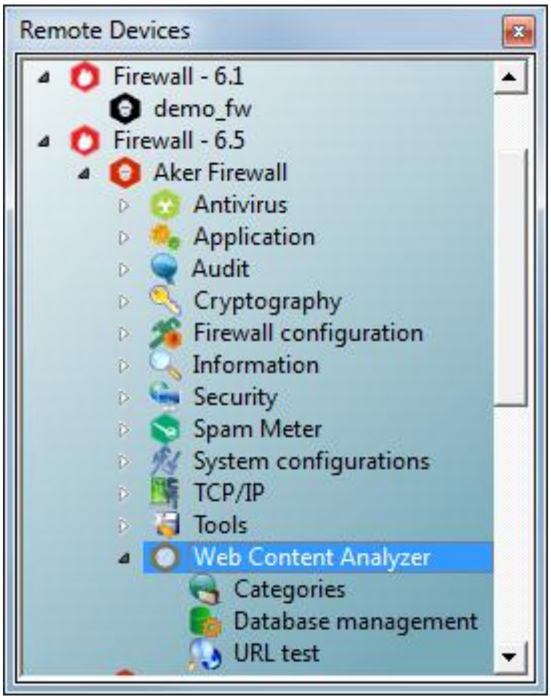

Remote Devices
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Categories
Database management
URL test

Image 591 – Aker Web Content Analyzer

On the Web Content Analyzer menu you will have 3 options, the description of each one of them follows below:

40.7. Database management

The **Database management** takes care of the malwares signatures updates.

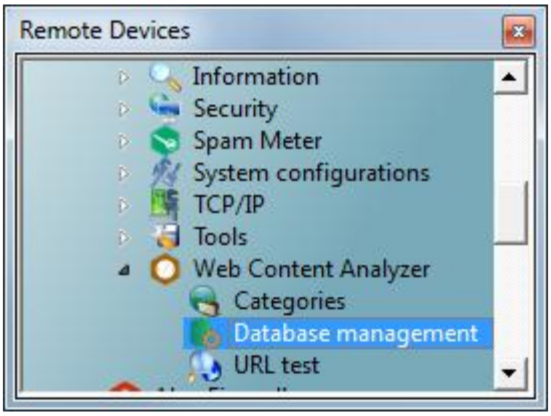
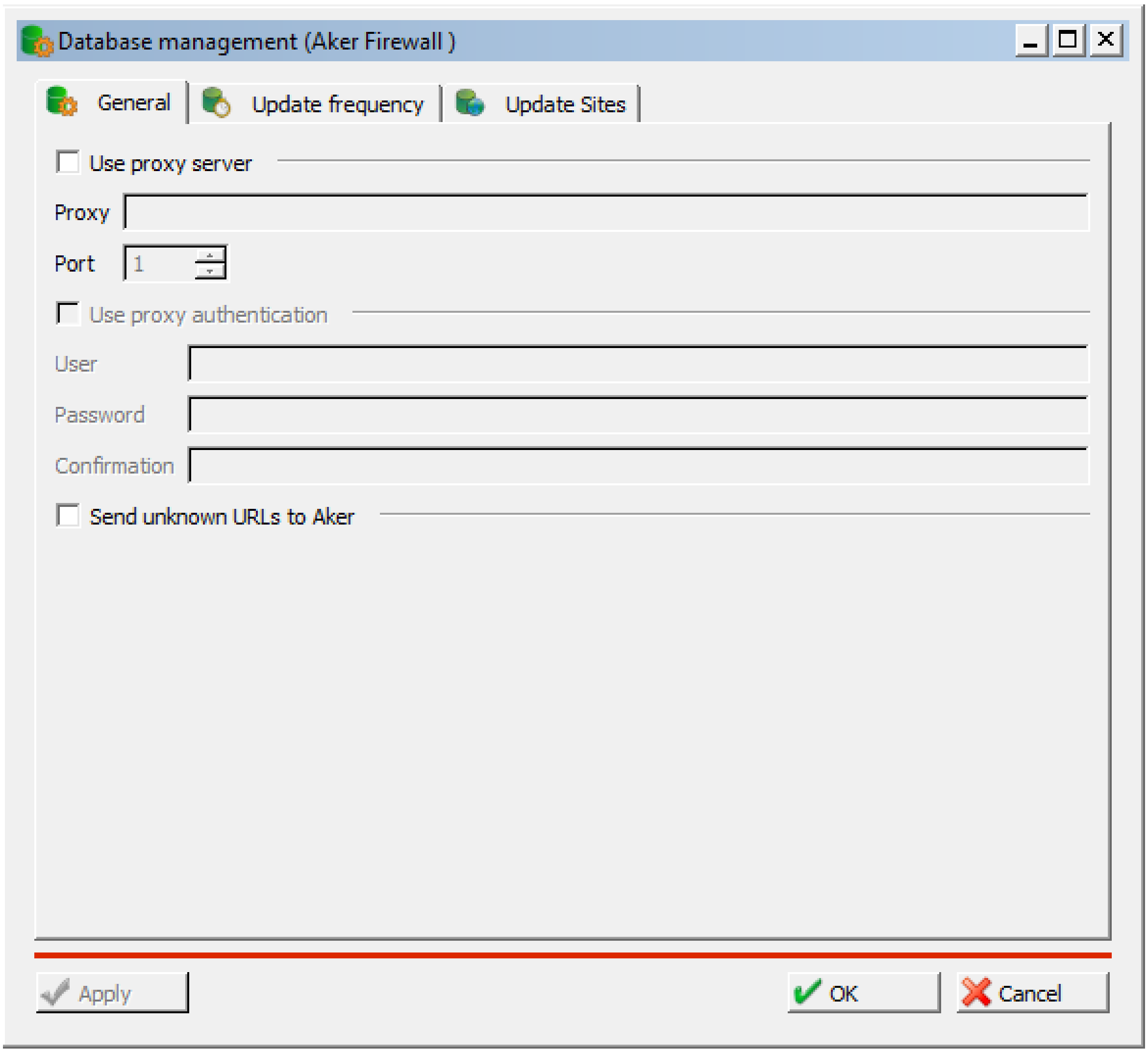

Remote Devices
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Categories
Database management
URL test

Image 592 – Access window: Database management

The database management has 3 tabs: **“General”**, **“update frequency”** and **“Update Sites”**.



Database management (Aker Firewall)
General
Update frequency
Update Sites

☐ Use proxy server

Proxy

Port 1

☐ Use proxy authentication

User

Password

Confirmation

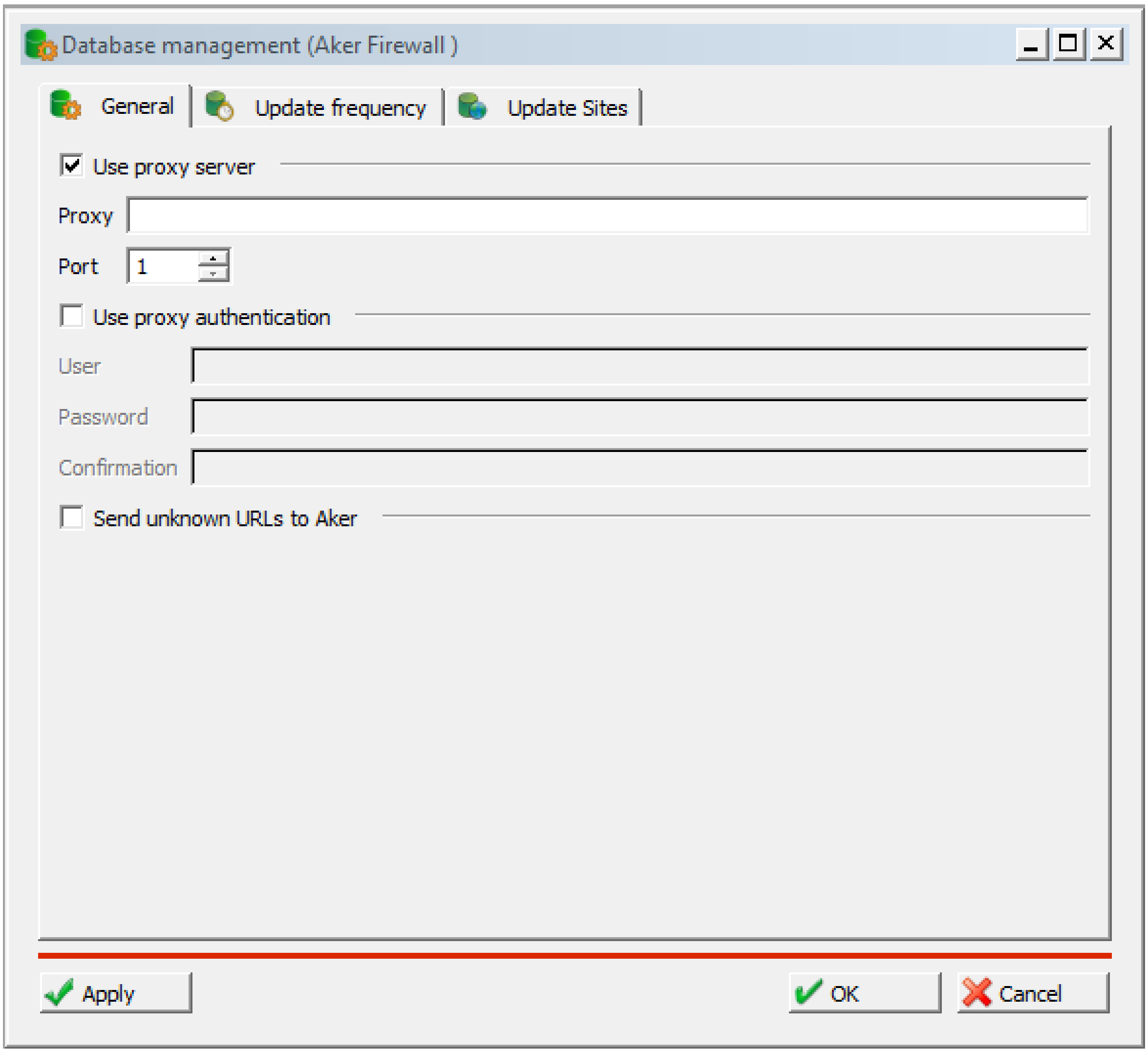
☐ Send unknown URLs to Aker

Apply
OK
Cancel

Image 593 – Menu: Database Management.

General tab

The signatures updates are made through the Internet. The required information to grant this access will be configured in this tab that is why **Aker Web Content Analyzer** needs to use or authenticate in any proxy to access the Internet.


Database management (Aker Firewall)
General
Update frequency
Update Sites
Apply
OK
Cancel

☑ Use proxy server

Proxy

Port 1

☐ Use proxy authentication

User

Password

Confirmation

☐ Send unknown URLs to Aker

Image 594 – Database management: General tab.

To perform the configuration the following fields need to be filled in:

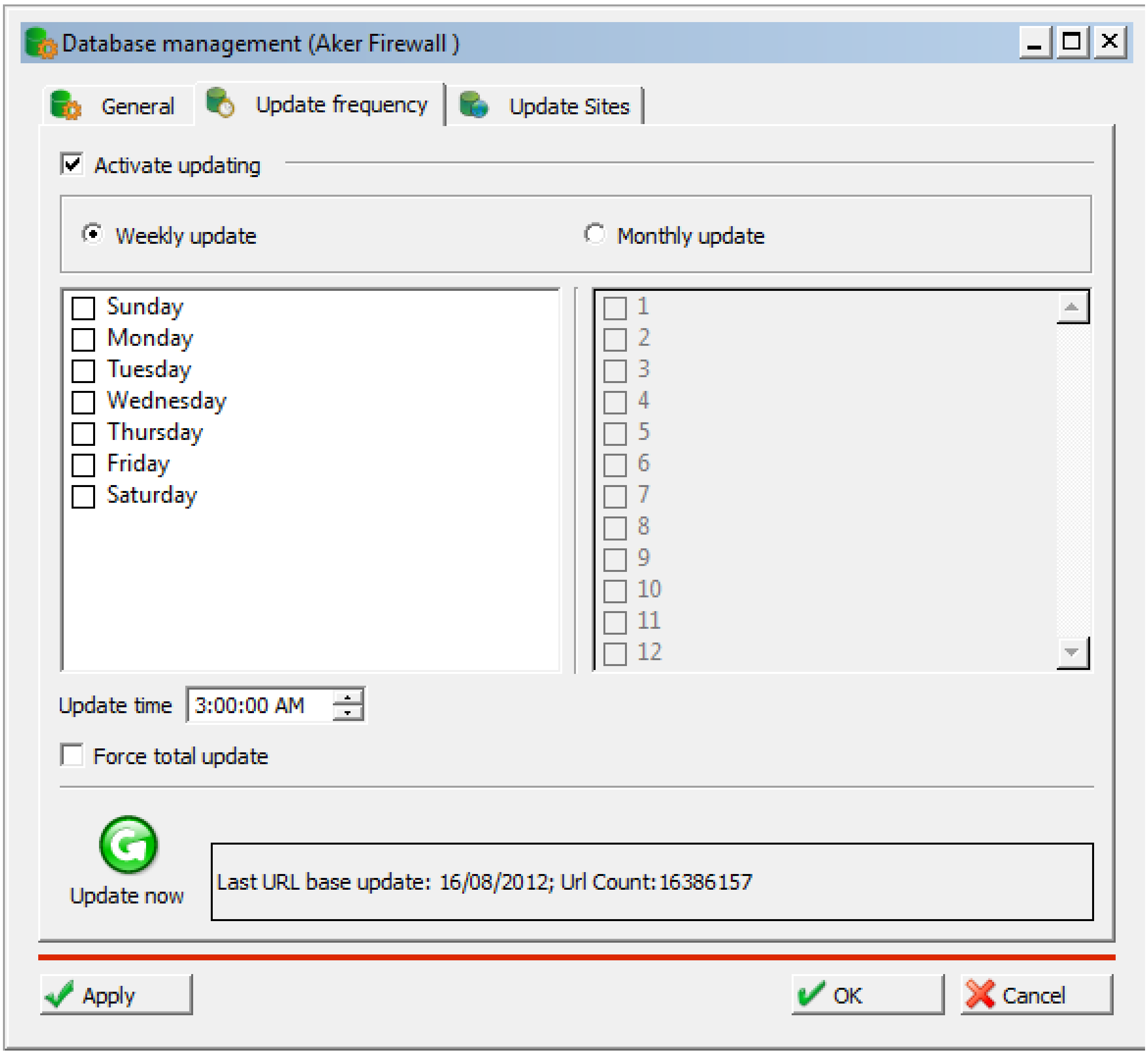
- Enable the option: Use proxy server;
- Proxy IP address and port;
- Enable the option: Use Proxy authentication;
- User and password.

Update frequency tab

The option **“Activate updating”** will enable or disable the automatic update. It is also possible to choose “**Weekly update** or **Monthly update**” according to the client’s need.

The URL’s signature update can be set to be performed automatically. In this tab the administrator can select week days or specific day of the month and the time that updates will be performed.

The **“Update Now”** button will perform the update at the moment you click on it.


Database management (Aker Firewall)
General
Update frequency
Update Sites
Update now
Apply
OK
Cancel

☑ Activate updating

● Weekly update ○ Monthly update

☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

☐ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10
☐ 11
☐ 12

Update time 3:00:00 AM

☐ Force total update

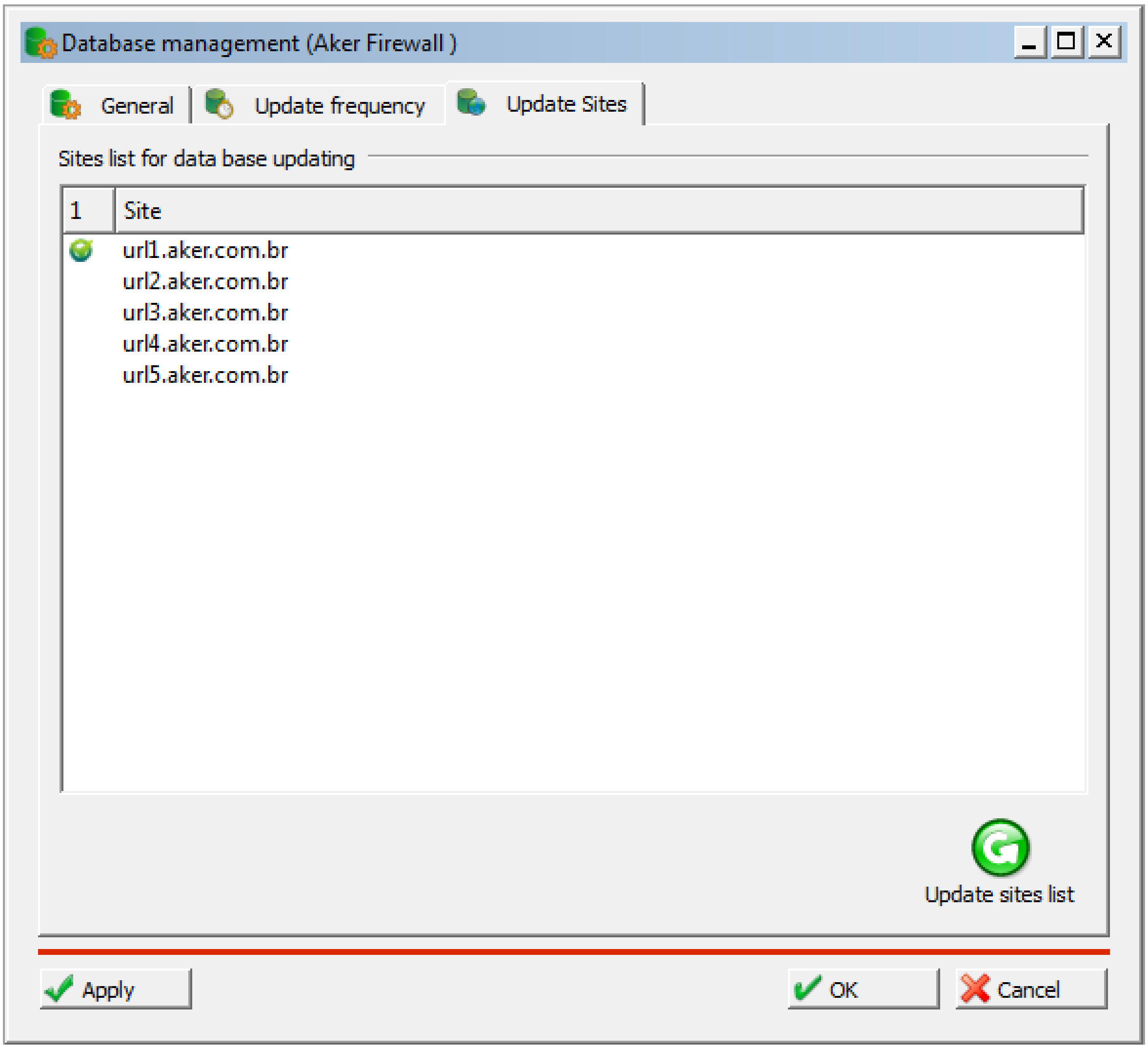
Last URL base update: 16/08/2012; Url Count: 16386157

Image 595 – Database management (Update frequency tab)

Once all configurations have been performed click on the **“Apply”** button.

Update sites tab

In this tab presents the websites that have URL signature base where the administrators will be able to update their signature. Clicking on the **"Update sites list"** button the system will search for configurations of the new websites that are available.


Database management (Aker Firewall)
General
Update frequency
Update Sites
Sites list for data base updating
1
Site
Update sites list
Apply
OK
Cancel

url1.aker.com.br
url2.aker.com.br
url3.aker.com.br
url4.aker.com.br
url5.aker.com.br

Image 596 – Database management (Update sites tab)

Once all configurations have been performed click on the **"Apply"** button.

Note: To update the URL database manually, follow the steps below:

1. Download the installer at www.aker.com.br;
2. Transfer the file to the appliance via SFTP to the server;
3. Access the appliance via ssh (text interface)
4. Execute the command line: Aker> awcabase

Usage: awcabase <base_file>

Example: awcabase base_awca.zip

40.8. Categories

This menu allows Aker Web Content Analyzer's administrator to modify the websites/URLs categories and create new categories.

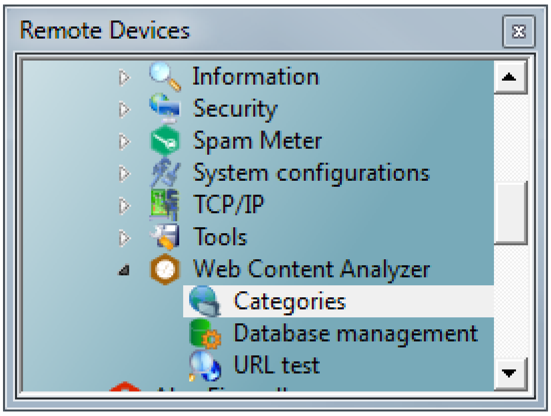

Remote Devices
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Categories
Database management
URL test

Image 597 – Access window: Categories.

The administrator can create his own categorization base in the following situations:

- When the administrator wishes to add any URL that is not categorized;
- When the administrator wishes to make a new configuration, in case he does not agreed with any URL/category that has been registered in the product signature database.
- When the administrator wishes to create new categories that are not registered on AWCA (Aker Web Control Analyzer).

The category can be made in two distinct levels: the *Father level* which is the main category, and the *Child level* which is the subcategory.

To create a new father category, the product's administrator need to right-click on the **"Categories"** menu and select the option **"New Category"**. To create a child category the product's administrator right-click on the desired category (father category) and select the option **"New Category"** then a child category will be created within the father category.

First example: creating a father category:

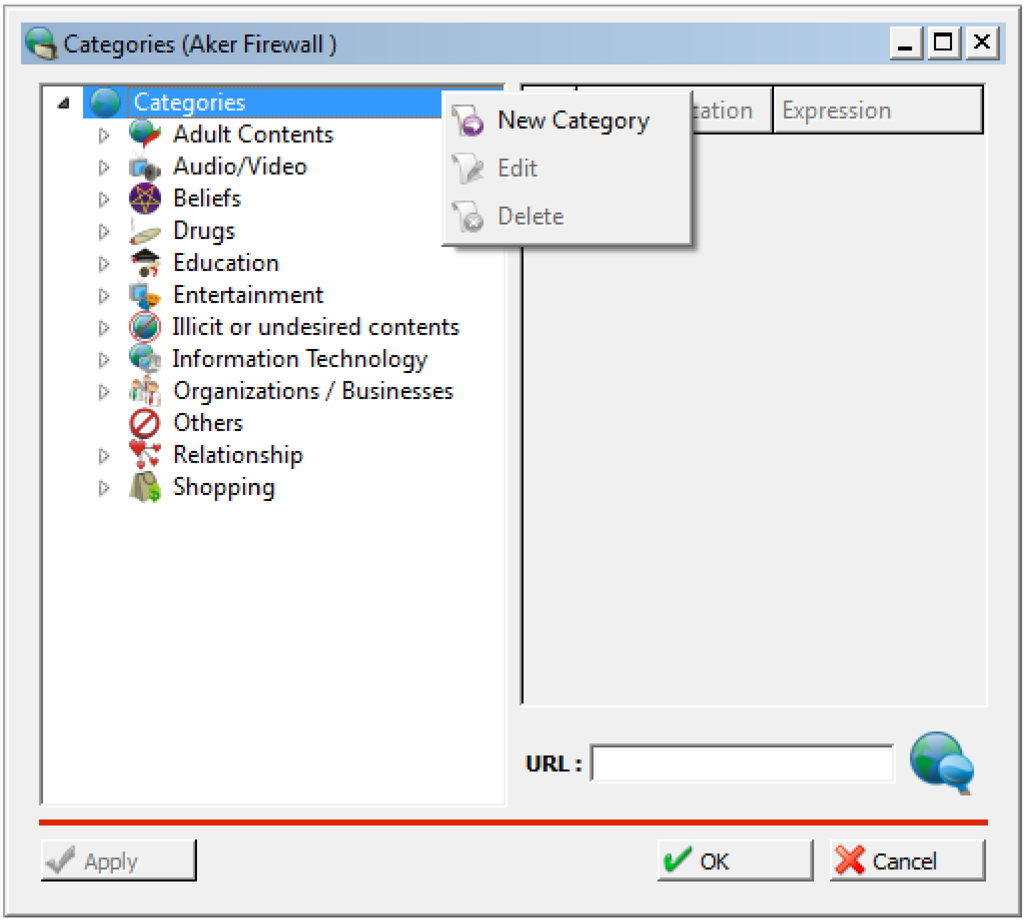

Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Information Technology
Organizations / Businesses
Others
Relationship
Shopping
New Category
Edit
Delete
ation
Expression
URL :
Apply
OK
Cancel

Image 598 – Creating a father category.

Second example: creating a child category:

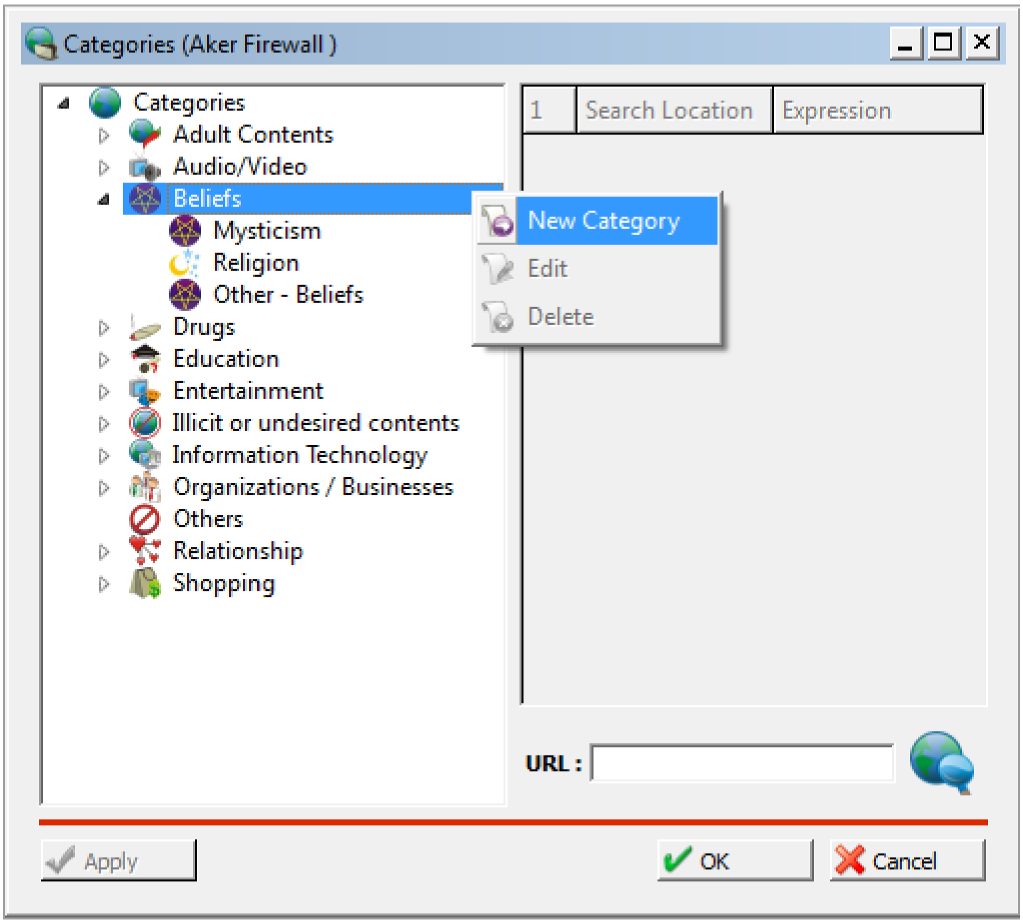

Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Mysticism
Religion
Other - Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Information Technology
Organizations / Businesses
Others
Relationship
Shopping
New Category
Edit
Delete
1
Search Location
Expression
URL :
Apply
OK
Cancel

Image 599 – creating a child category.

After filling in the fields to the category creation click on the icon button displayed below to select a specific icon to your new category.

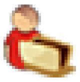


Image 600 – Icon button.

The following screen will be displayed:

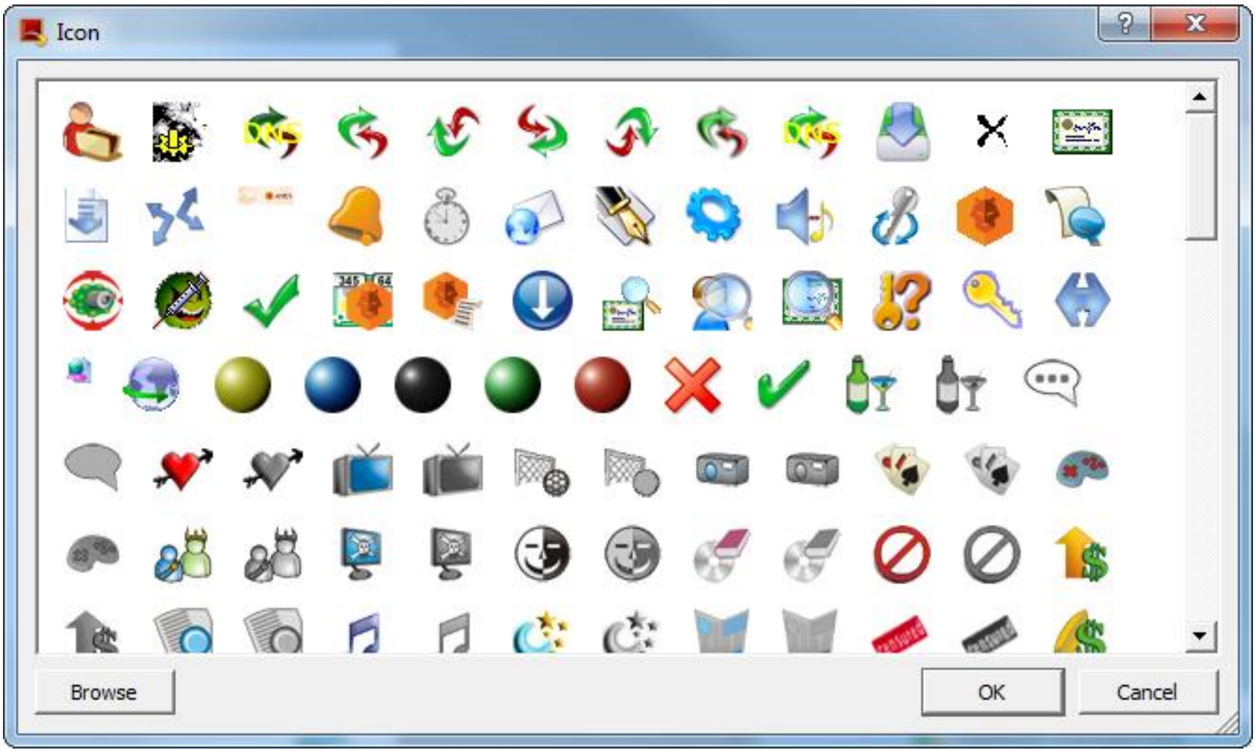

Icon
Browse
OK
Cancel

Image 601 – Choosing the category icon.

After selecting the icon to your category click on **“OK”**

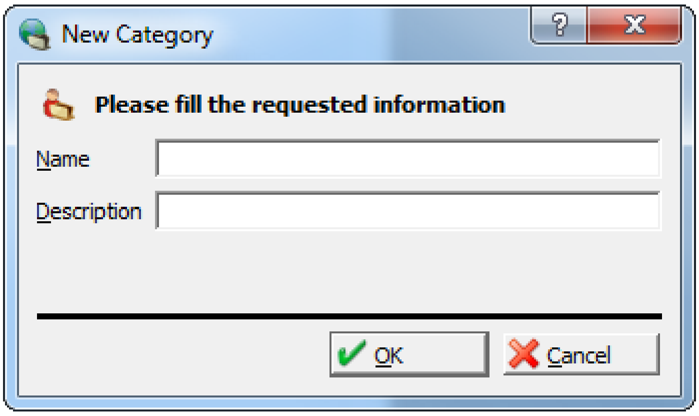

New Category
Please fill the requested information
Name
Description
OK
Cancel

Image 602 – New category window.

Requested information:

- **Name:** Category’s name;
- **Description:** A brief summary of the website content;

Below follows an example:

- **Category**: Education;
- **Description**: Educational organization websites or in some way contributes the education publicizing.

User can use icons provided by AWCA or any other icon, since it is 32 by 32 pixels and it is on "png." format.

After creating a category is necessary to create a list of expressions. The categories with registered expressions will appear in bold. To create this list, the product's administrator need to select the desired category and right-click on the black area as the example below, the option are search location and expression:

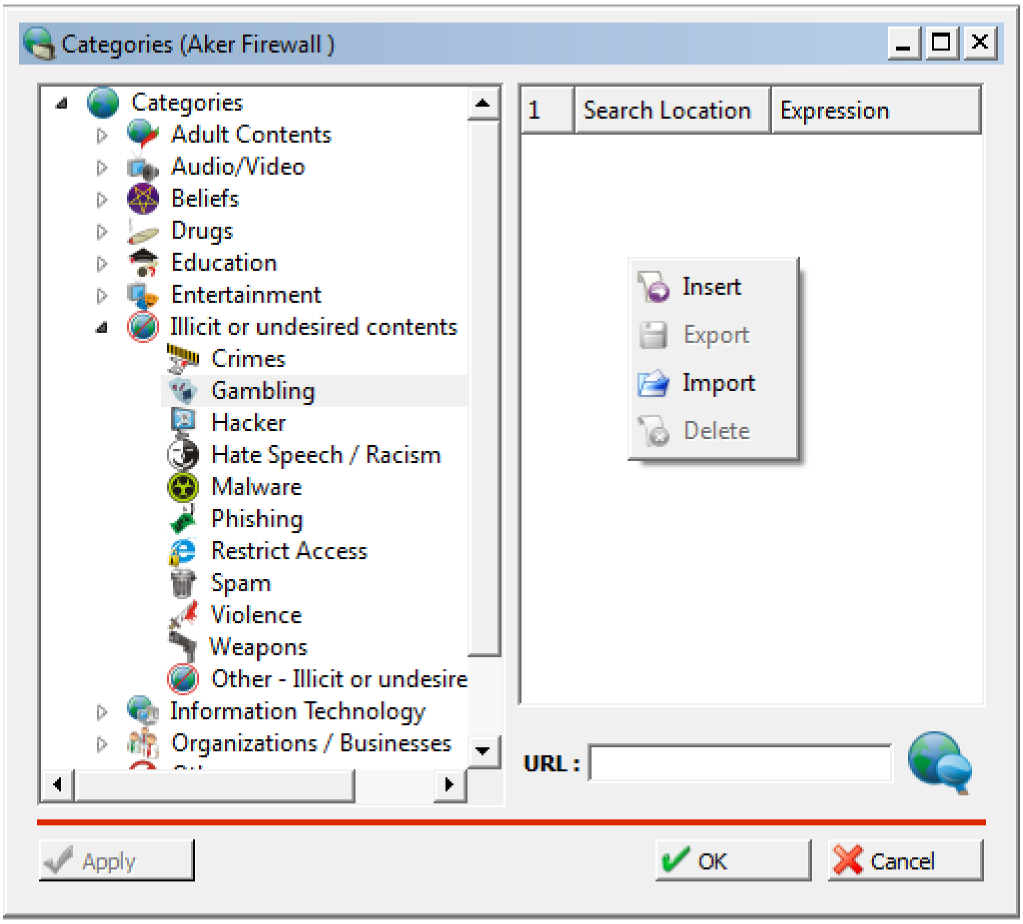

Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Crimes
Gambling
Hacker
Hate Speech / Racism
Malware
Phishing
Restrict Access
Spam
Violence
Weapons
Other - Illicit or undesire
Information Technology
Organizations / Businesses
1
Search Location
Expression
Insert
Export
Import
Delete
URL :
Apply
OK
Cancel

Image 603 – Expression list creation.

- **Expression:** Defines which string or parameters will be searched at the accessed URL, and which operation will be performed. The operation can have different types, e.g. "*Aker*" (contains), "Aker" (is), "*Aker" (ends with), "Aker*" (begins with).

Each entry in the expression list of the category window:

***** stands for any amount of characters, including none
? stands for one character
\ * and the character *
\? And the character ?
\\ and the character \

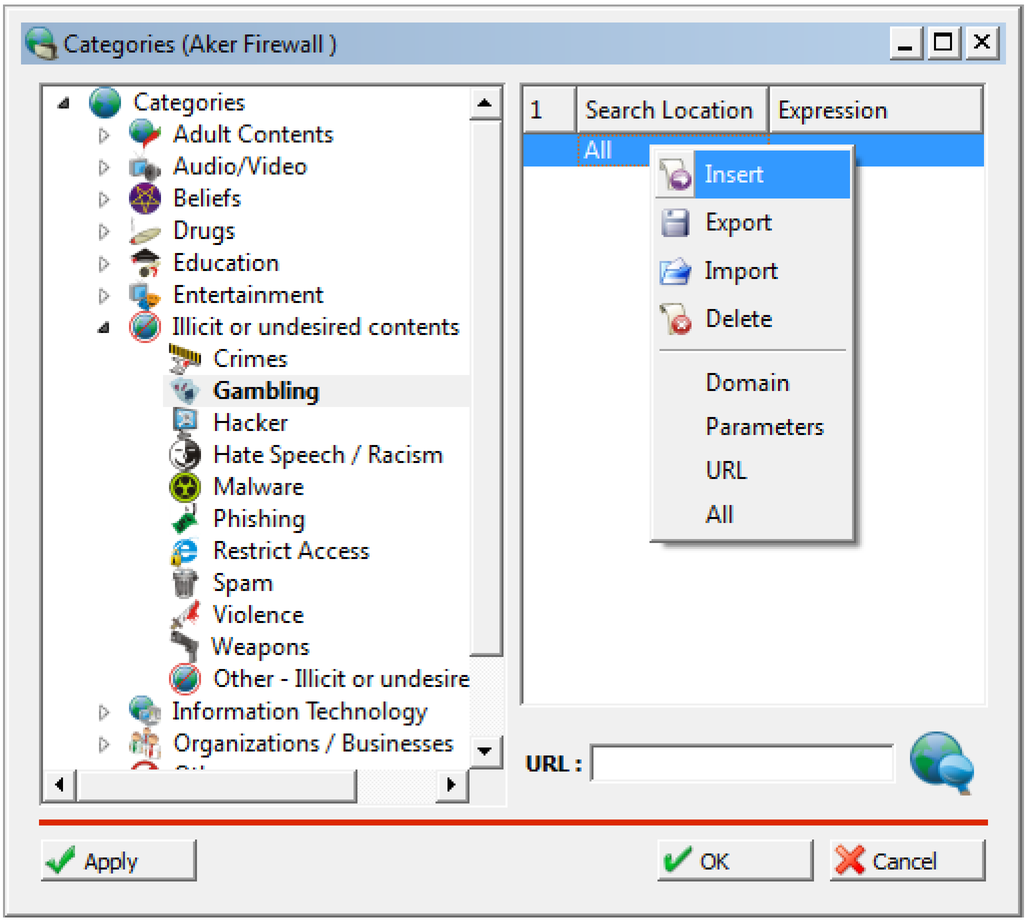

Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Crimes
Gambling
Hacker
Hate Speech / Racism
Malware
Phishing
Restrict Access
Spam
Violence
Weapons
Other - Illicit or undesire
Information Technology
Organizations / Businesses
1
Search Location
Expression
All
Insert
Export
Import
Delete
Domain
Parameters
URL
All
URL :
Apply
OK
Cancel

Image 604 – Option menu

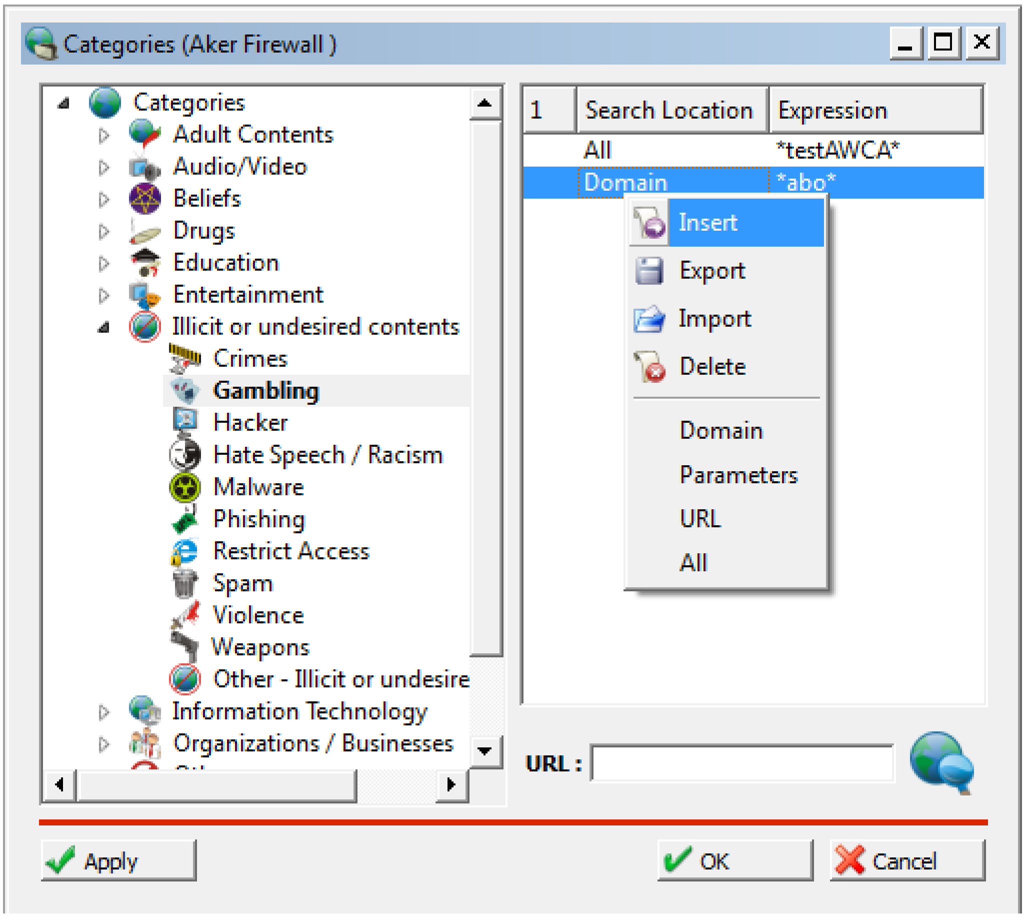
- **Search Location:** Sets the specific place of the query on the websites. Right-clicking on this option user will be able to set 4 different ways to query.

Below follows the example of how to fill in these fields:

http://www.aker.com.br/index.php?pag_cod=1&ling=pt_br

- **Domain:** Performs the search at the domain : www.aker.com.br
- **Parameters:** Performs the search on the website parameters: pag_cod=1&ling=pt_br
- **All:** Performs the search on the entire URL: www.aker.com.br/index.php?pag_cod=1&ling=pt_br

- **URL:** Performs the search only on the URL: www.aker.com.br/index.php

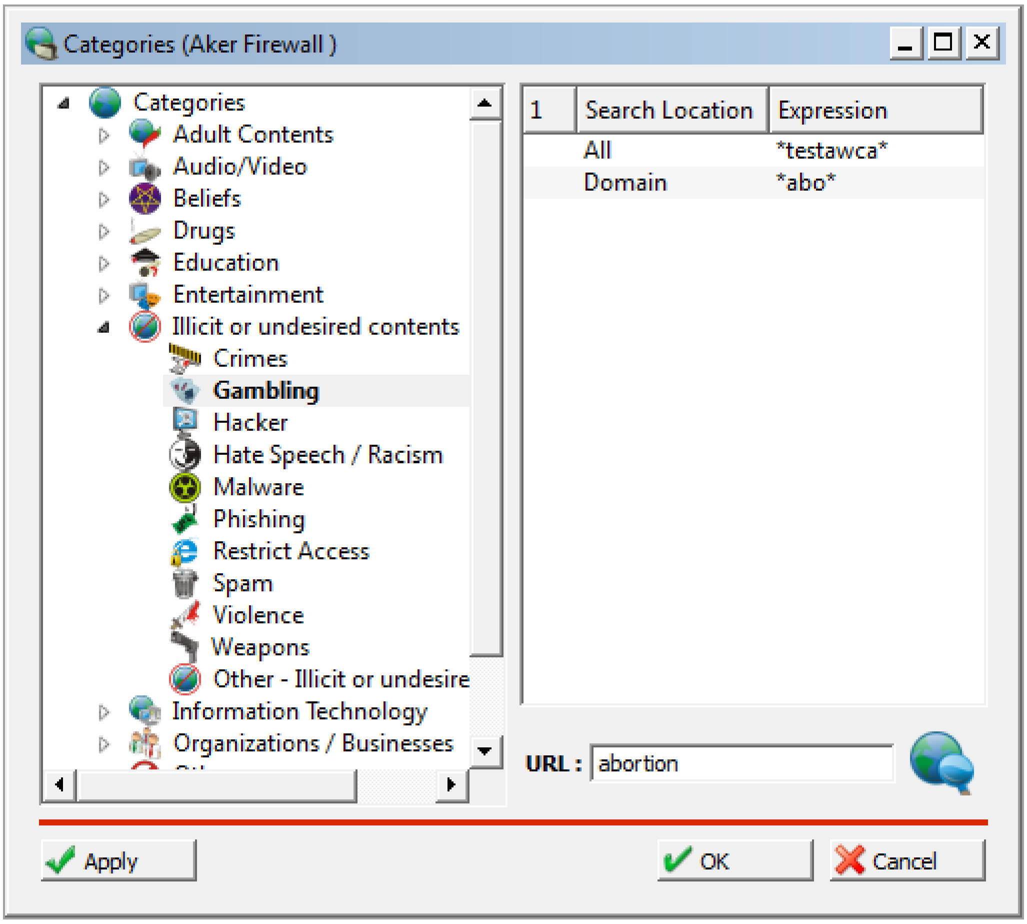

Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Crimes
Gambling
Hacker
Hate Speech / Racism
Malware
Phishing
Restrict Access
Spam
Violence
Weapons
Other - Illicit or undesire
Information Technology
Organizations / Businesses
Insert
Export
Import
Delete
Domain
Parameters
URL
All
URL :
Apply
OK
Cancel

1	Search Location	Expression
	All	*testAWCA*
	Domain	*abo*

Image 605 – Search Location menu

To confirm if the expressions that have been set and check if they are working, on the “URL” field type a word, and click on the search button to verify if the word you have typed does or not match in the expressions.

Image 606 – Search button.


Categories (Aker Firewall)
Categories
Adult Contents
Audio/Video
Beliefs
Drugs
Education
Entertainment
Illicit or undesired contents
Crimes
Gambling
Hacker
Hate Speech / Racism
Malware
Phishing
Restrict Access
Spam
Violence
Weapons
Other - Illicit or undesire
Information Technology
Organizations / Businesses
Apply
OK
Cancel

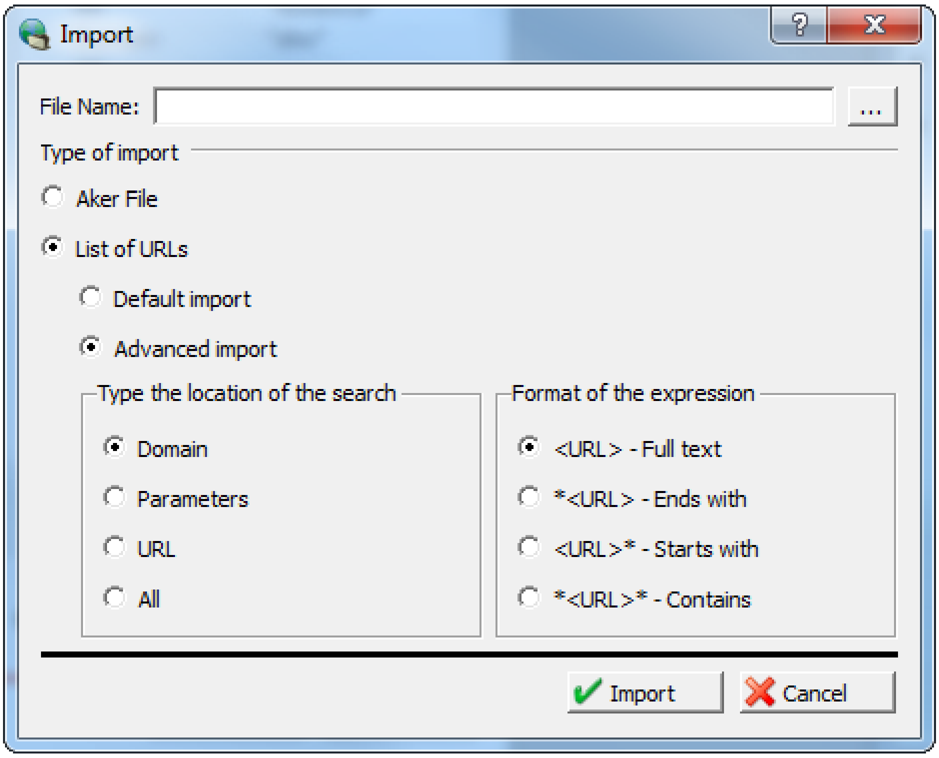
1	Search Location	Expression
	All	*testawca*
	Domain	*abo*

URL : abortion

Image 607 – Categories

Creating expressions the users have the export and import features, facilitating the migration of other URLs database to Aker's database.

- **Export expressions:** In case there is a category the user can export them to a file. To export the expressions of a category right-click on the expression list and select the option **"Export"**, choose the location and a name to the file, then click on **"Save"**. Aker Control Center will save the expressions as ".exps" extension.
- **Import expressions:** To import expressions simply right-click and select the option **"import"** and a window will be displayed to select the file to be imported. There are two ways to import expressions; the first on is through a file exported of a category or import it from a file containing a list of URLs (one URL per line).



Import

File Name:

Type of import

○ Aker File

● List of URLs

○ Default import

● Advanced import

Type the location of the search

● Domain

○ Parameters

○ URL

○ All

Format of the expression

● <URL> - Full text

○ *<URL> - Ends with

○ <URL>* - Starts with

○ *<URL>* - Contains

Image 608 – Import file.

The window presents the following information:

File Name: File that will be imported location and name (with extension);

Type of import: Indicates from which file the import will be made. Below follows the description of its option:

- **Aker file:** Imports from an exported file of a category. The file shall have ".exps" extension;
- **List of URLs:** Imports from a text file containing a URL per line. The import through URL list has two options:
- **Default import:** Imports the file URL creating expressions, performing the search at the URL domain and expression format in **“full text”**;
- **Advanced import:** Allows the user to select the location and type of search and the expression format that will be applied to all file’s URLs. Below follows the description of the advanced options:

Search location type:

- **Domain:** Select all expressions to perform the search at the URL domain;
- **Parameters:** Select all expressions to perform the search on the URL parameters;
- **URL:** Select all expressions to perform the search on the URL;
- **All:** Select all expressions to perform the search in all fields of the URL.
- **Format of the expression:**

- **Full text:** all URLs will be added as they are in the file (to perform the search on everything that is equal to URL). E.g. <url>
- **Ends with:** an * (asterisk) will be added at the beginning of each URL imported from the file (to perform the search on everything that ends with the URL). E.g. <url>
- **Start with:** an * (asterisk) will be added at the end of all URLs imported from the file (to perform the search on everything that starts with the URL). E.g. <url>
- **Contains:** an * (asterisk) will be added at the end, and at the beginning of all URLs imported from the file (to perform the search on everything that contains the URL). E.g. <url>

After importing the file and the import type click on **“Import”** and Aker Control Center will import all file’s expressions. At the end a summary of the importation will be presented containing information such as:

- Total number of expressions on the file;
- Total number of expressions that were already in the file;
- Existing categories;
- Total number of imported expressions and the total number of expressions that could not be imported because they presented errors.
- Containing expressions with errors, a list with all expressions that have errors, which can be copied to other files, fixed and imported again will be presented;

Users can export and import the complete list of categories and their expressions:

- **Export button:** Saves the categories customizations, working as a form of backup to a future recovery, or to use it on another Aker Web Content Analyzer;
- **Import button:** Retrieve exported categories.

40.9. URL test

This menu is composed of a list of icons with categories names which the URL test matches.

To gain access to the URL test window follow the steps below:

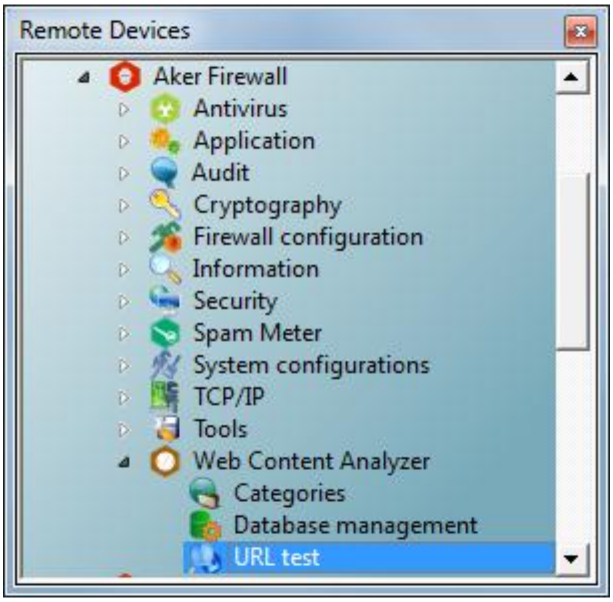

Remote Devices
Aker Firewall
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
System configurations
TCP/IP
Tools
Web Content Analyzer
Categories
Database management
URL test

Image 609 – URL test

- Click on the *Web Content Analyzer* menu
- Select URL test

The following window will be displayed:

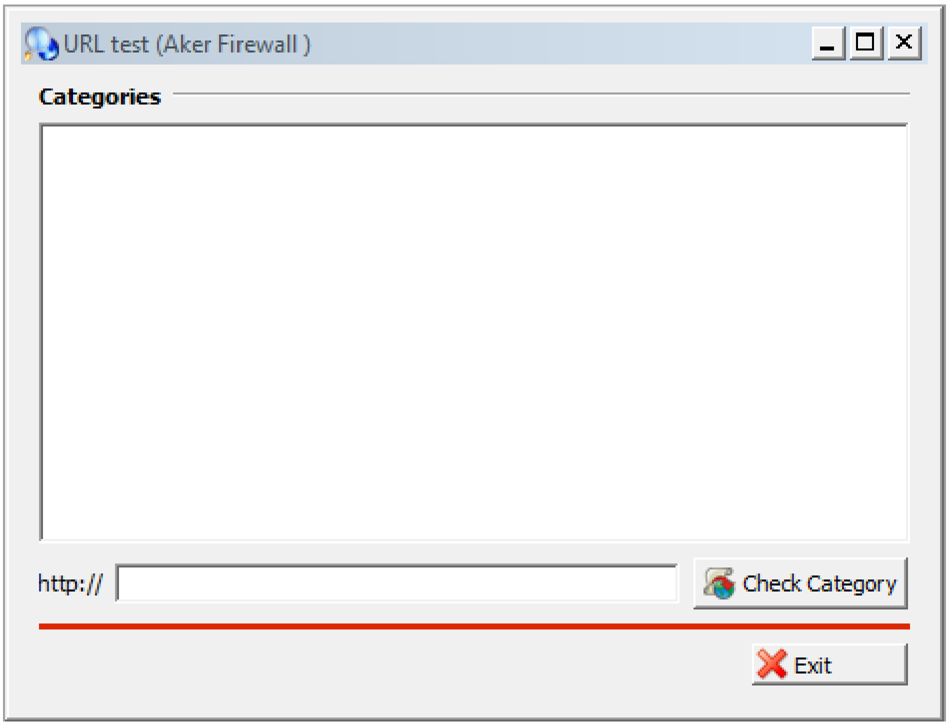

URL test (Aker Firewall)
Categories
http://
Check Category
Exit

Image 610 – URL test.

Typing the URL name (at the http:// filed) and clicking on **“Check Category”**, the product will inform which is the URL category and show its corresponding icon. In case the URL is not associated to any category the message **“not found”** will be displayed**.**

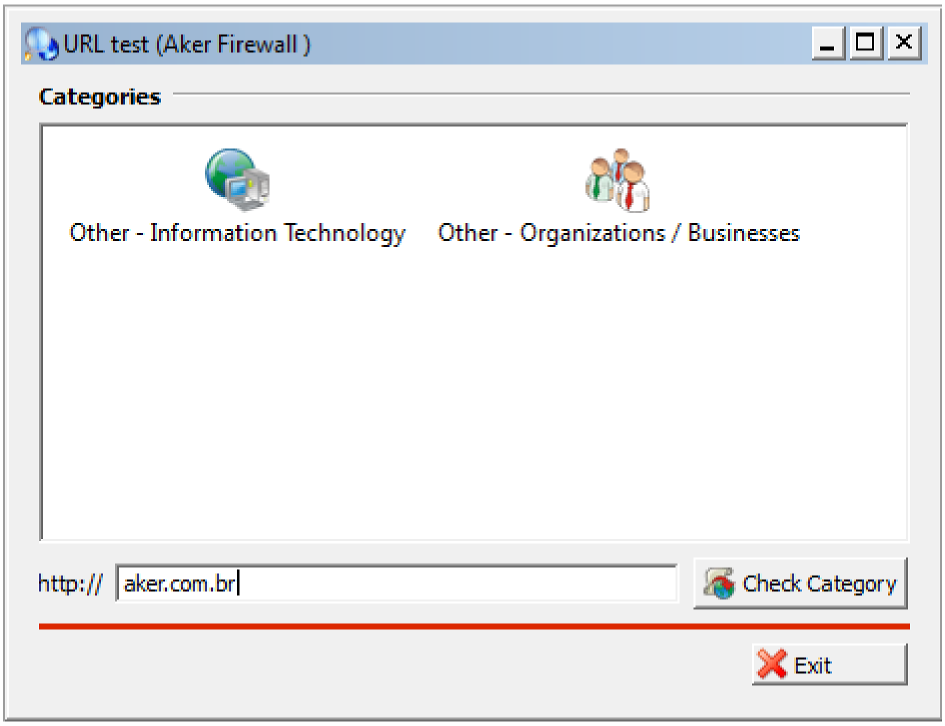

URL test (Aker Firewall)
Categories
Other - Information Technology
Other - Organizations / Businesses
http://
aker.com.br
Check Category
Exit

Image 611 – Categorized URL test.

After the query simply click on the **“exit”** button.

Manual do Plugin – ASM
Aker Spam Meter

41. Aker Spam Meter – ASM

This chapter shows how to install and use ASM on Aker Firewall.

41.1. Introduction

Spam is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, social spam, television advertising and file sharing network spam.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions.

Instant messaging spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, according to a report from Ferris Research, 500 million spam IMs were sent in 2003, twice the level of 2002. As instant messaging tends to not be blocked by firewalls, it is an especially useful channel for spammers. This is very common on many instant messaging systems such as Skype.

Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family. As for Twitter, spammers gain credibility by following verified accounts such as that of Lady Gaga; when that account owner follows the spammer back, it legitimizes the spammer and allows him or her to proliferate.

Email spam, also known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Spam in email started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today composes some 80 to 85% of all the email in the world, by a "conservative estimate". Pressure to make email spam illegal has been successful in some jurisdictions, but less so in others. Spammers take advantage of this fact, and frequently outsource parts of their operations to countries where spamming will not get them into legal trouble.

Increasingly, email spam today is sent via "zombie networks", networks of virus- or worm-infected personal computers in homes and offices around the globe. Many modern worms install a backdoor that allows the spammer to access the computer and use it for malicious purposes. This complicates attempts to control the spread of spam, as in many cases the spam does not obviously originate from the spammer.

41.2. Presenting ASM (Aker Spam Meter)

Aker spam meter allows each person or group to classify their email according to their profile, allowing the product to learn what this person or group wants to receive. One of the major difficulties when trying to deal with this problem is, defining what is junk mail, since the internet has a large number of users that have different views about a specific topic. An email received and read by a person on a particular subject may not be of interest to another, and so on. When opening your mail box to read your emails, all users face a large amount of unwanted messages such as advertisements, chain letters, pornography, and even programs attackers disguised as legitimate email messages daily.

41.3. How does the classification work

The product analyses the email content, based in statistic database, i.e. assign a grade for each message based in statistic database that are generated through thousands of messages in different languages, pre-classified in spam or not spam. As larger the messages database used to generate the statistic database and as much the files be specified, better will be the result.

To Aker Spam Meter is extremely fast and has two distinct databases to better classify the messages; one is generated by Aker and it is updated daily, the other is produced through the training made by each user or group. Combining databases, Aker and users/groups the system reaches a high level of classification.

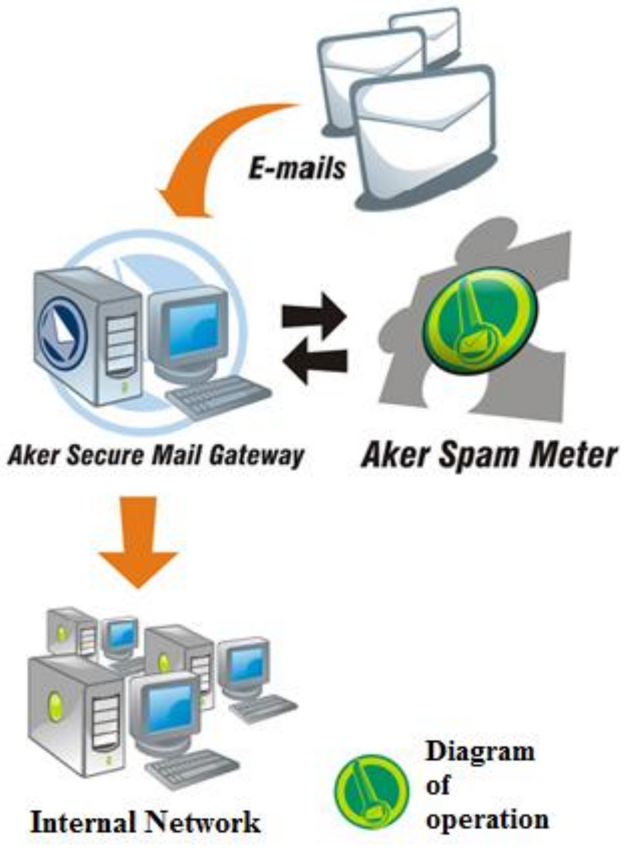

E-mails
Aker Secure Mail Gateway
Aker Spam Meter
Internal Network
Diagram
of
operation

Image 612 – Aker Spam Meter: Diagram of operation.

41.4. Aker Control Center

Aker Spam Meter is remotely controlled by Aker Control Center which is an appliance that controls all solutions of Aker Security Solutions.

Remote Device

To gain access to the Spam Meter menu follow the steps below**:**

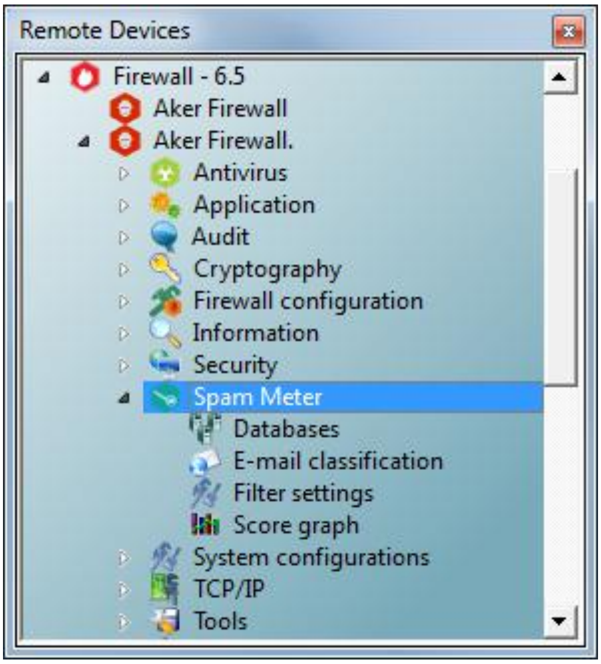

Remote Devices
Firewall - 6.5
Aker Firewall
Aker Firewall.
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
Databases
E-mail classification
Filter settings
Score graph
System configurations
TCP/IP
Tools

Image 613 – Access window: Spam Meter.

- Open **Aker Control Center**, and select the desired Firewall
- Select the **Spam Meter** menu

Aker Spam Meter has 4 options: **Databases, E-mail classification, Filter settings, Score graph**. The description of each one of them follows below:

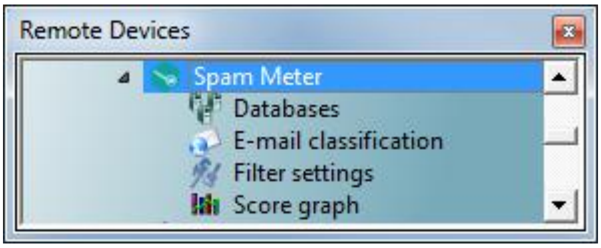

Remote Devices
Spam Meter
Databases
E-mail classification
Filter settings
Score graph

Image 614 – Spam Meter menu.

41.5. Databases

The Databases menu has the e-mails database configuration and their classification.

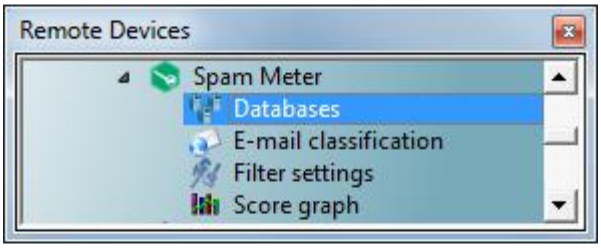
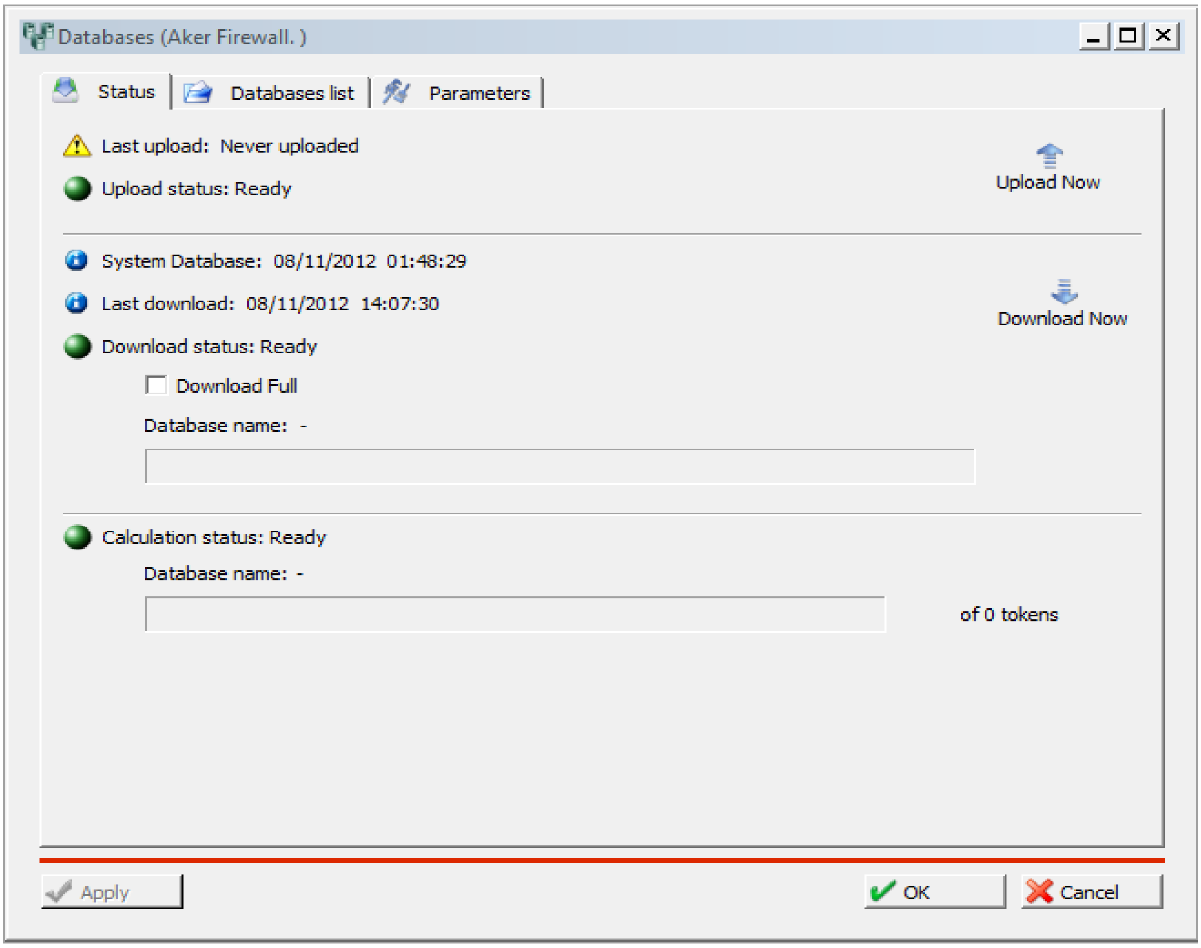

Remote Devices
Spam Meter
Databases
E-mail classification
Filter settings
Score graph

Image 615 – Access window: Databases.

The Databases menu has the following tabs: **Status, Databases list** and **Parameters**. The description of each of them follows below:



Databases (Aker Firewall.)
Status
Databases list
Parameters
Upload Now
Download Now
Apply
OK
Cancel

Last upload: Never uploaded

Upload status: Ready

System Database: 08/11/2012 01:48:29

Last download: 08/11/2012 14:07:30

Download status: Ready

☐ Download Full

Database name: -

Calculation status: Ready

Database name: -

of 0 tokens

Image 616 – Databases window.

Status tab:

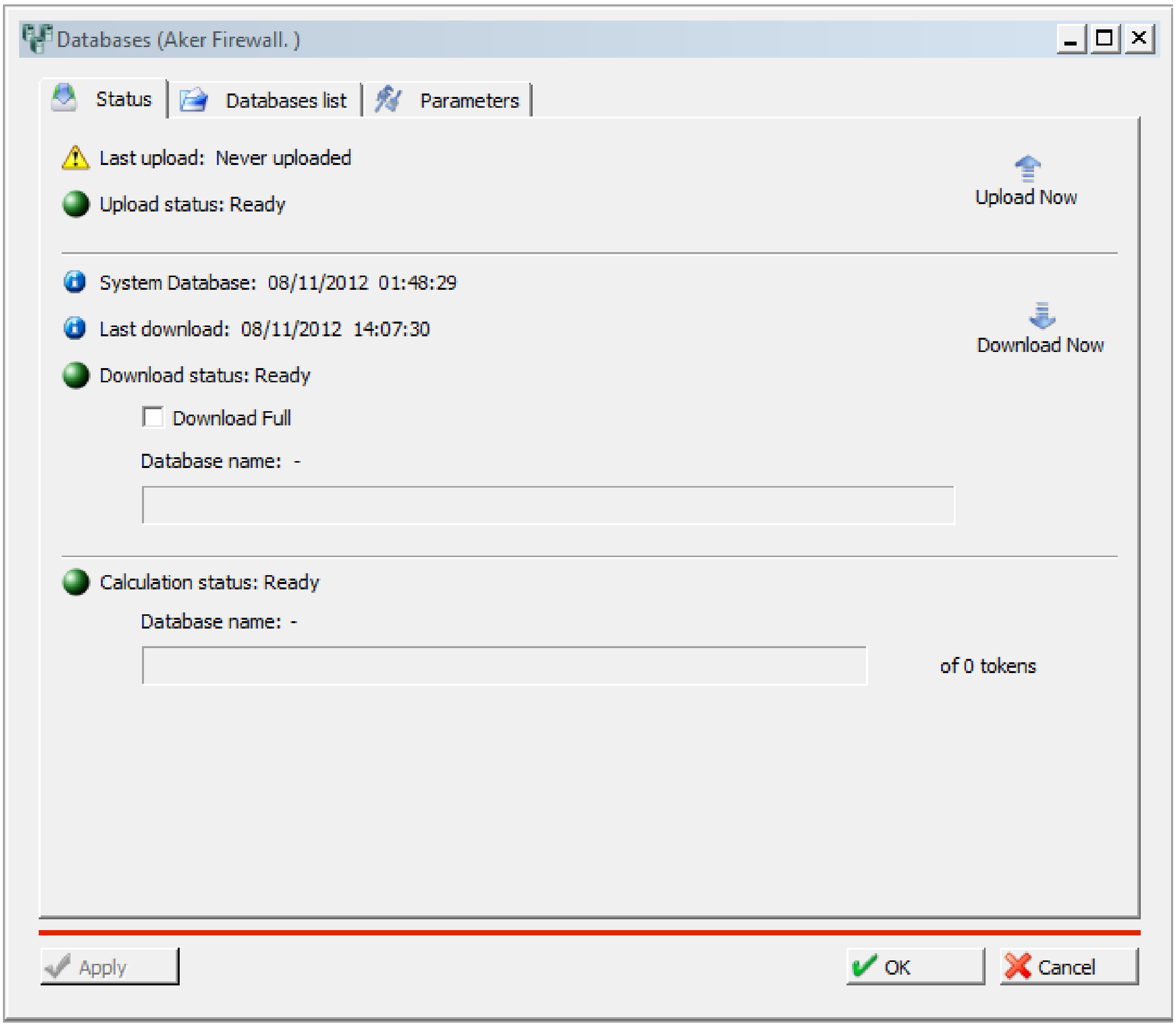
The **“Status tab”** presents information about the databases’ download and uploads current status.

Uploads are emails manually classified by users who can or not be sent to Aker in order to improve the email classification of emails and signatures database.

The **“Download now”** button downloads the most recently email signature database.

Databases list tab:

The **“Databases list tab”** presents all existing database in the system, its status and database size.


Databases (Aker Firewall.)
Status
Databases list
Parameters
Upload Now
Download Now
Apply
OK
Cancel

Last upload: Never uploaded

Upload status: Ready

System Database: 08/11/2012 01:48:29

Last download: 08/11/2012 14:07:30

Download status: Ready

☐ Download Full

Database name: -

Calculation status: Ready

Database name: -

of 0 tokens

Image 617 – Databases list tab

This menu has two options; **“Save Backup”** and **“Restore Backup”**. These options allow the Administrator to make copies of emails/classification database and its later restoration if necessary. The copy or the restore are performed by clicking on the following buttons:

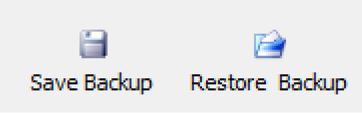

Save Backup
Restore Backup

Image 618 – Buttons: Save Backup and Restore Backup.

The database update, its recalculation (information regarding to the emails punctuation) or its exclusion can be made by using the following buttons:

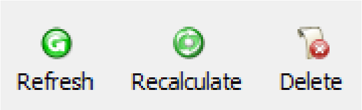
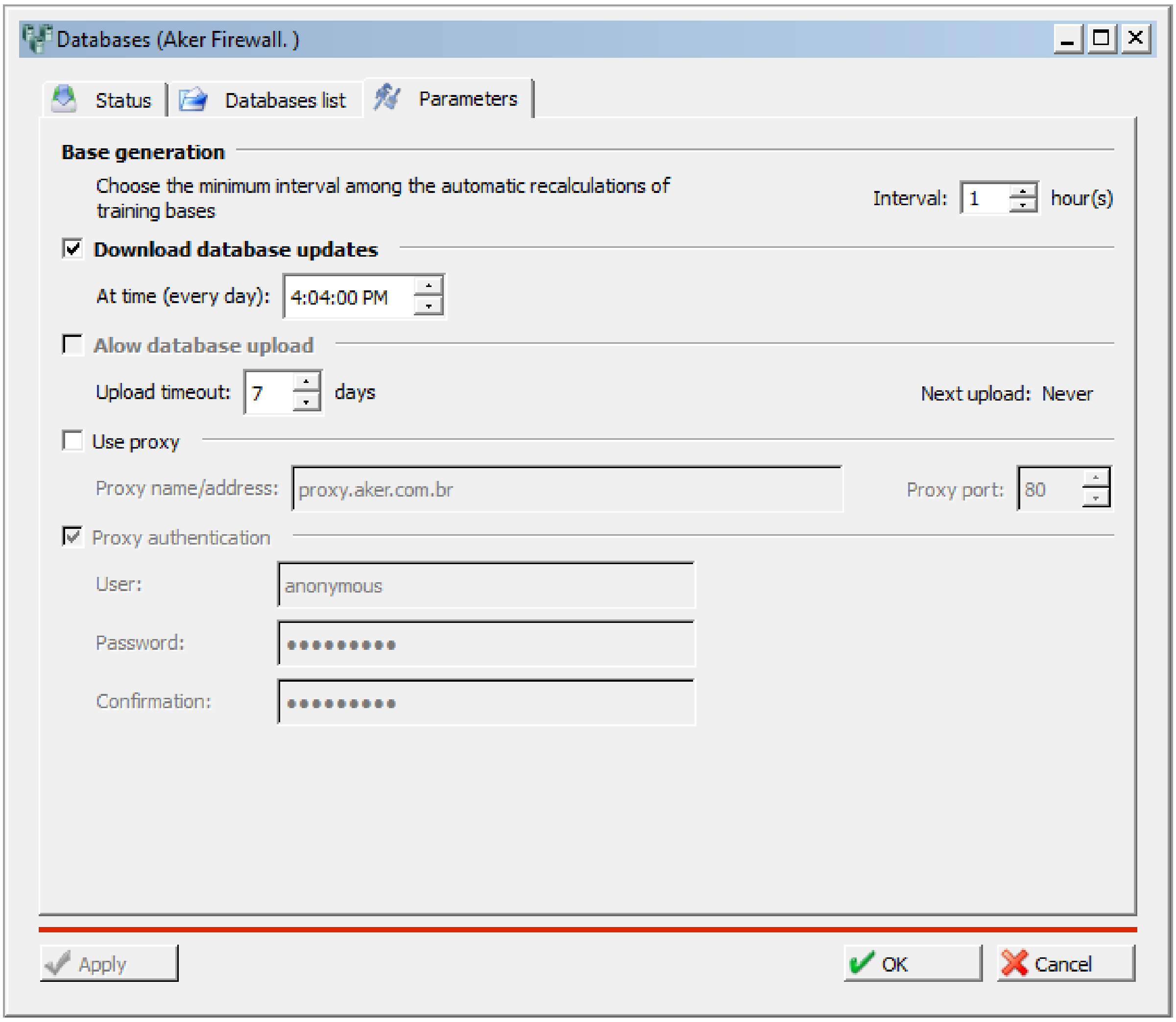

Refresh
Recalculate
Delete

Image 619 – buttons: Refresh, recalculate and delete.

Parameters tab

The **“Parameters tab”** presents the configuration required for the automatic generation and updates of databases.



Base generation

Choose the minimum interval among the automatic recalculations of training bases

Interval: 1 hour(s)

☑ **Download database updates**

At time (every day): 4:04:00 PM

☐ **Alow database upload**

Upload timeout: 7 days

Next upload: Never

☐ Use proxy

Proxy name/address: proxy.aker.com.br

Proxy port: 80

☑ Proxy authentication

User: anonymous

Password: ●●●●●●●●●

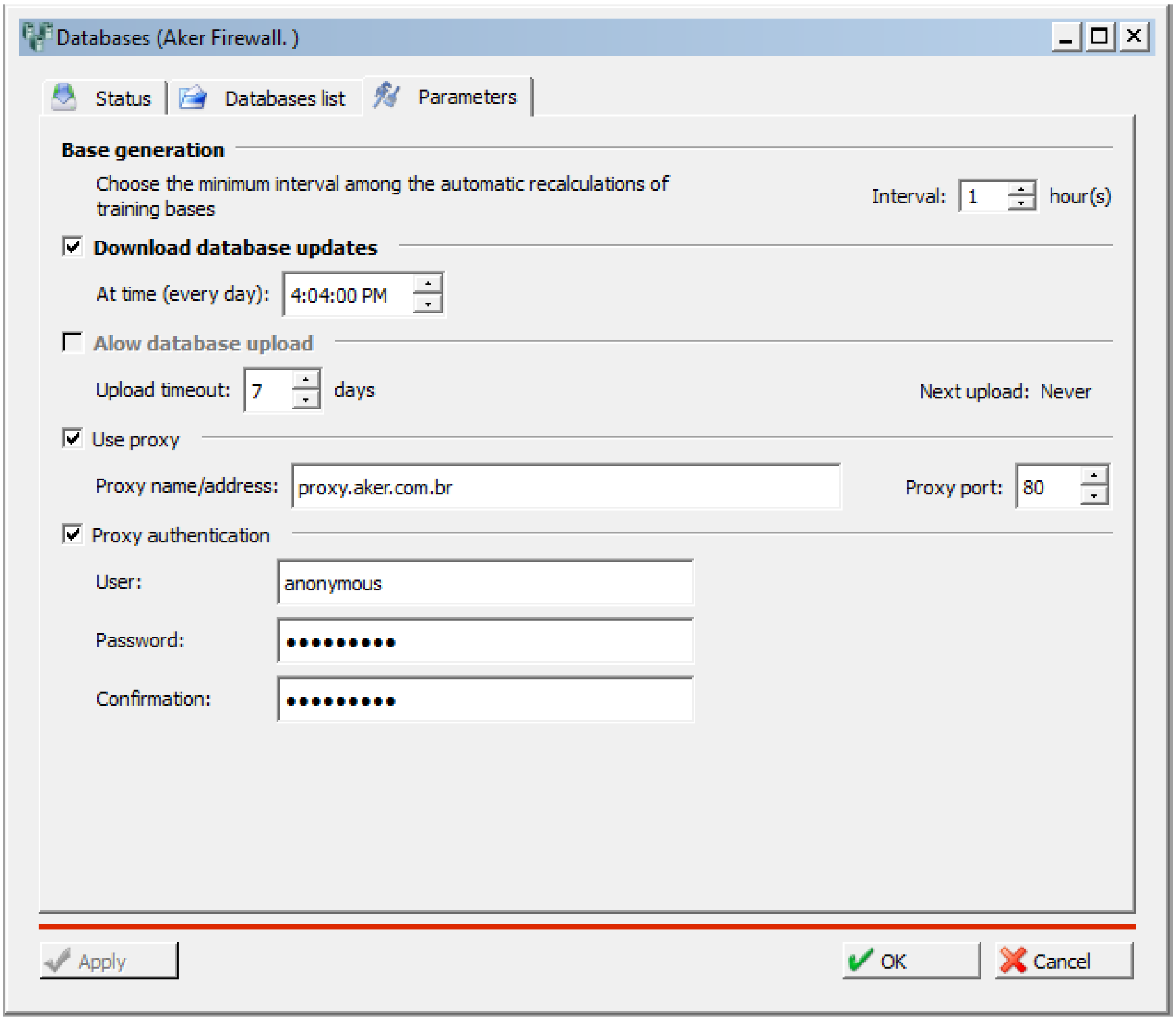
Confirmation: ●●●●●●●●●

Image 620 – Parameters.

Below follows the description of the options presented in the window above:

- **Base generation:** Chooses the minimum interval among the automatic recalculations of training bases.
- **Download database updates:** This option configures the server that provides the database to be downloaded as the time that Aker Spam Meter will download database updates.
- **Allow database upload:** In case the administrator wishes to send Aker the email database manually, he can do it using the **"Upload now"** button on the **Status tab** or configuring the automatic sending through this option and setting the interval timeout (weekly)

The update of email/classification databases are made through the Internet. In case Aker Spam Meter needs to use or authenticate itself in any proxy to access the Internet, the required information to allow this access will be configured in this tab.



Base generation

Choose the minimum interval among the automatic recalculations of training bases

Interval: 1 hour(s)

☑ **Download database updates**

At time (every day): 4:04:00 PM

☐ **Alow database upload**

Upload timeout: 7 days

Next upload: Never

☑ Use proxy

Proxy name/address: proxy.aker.com.br

Proxy port: 80

☑ Proxy authentication

User: anonymous

Password: •••••••••

Confirmation: •••••••••

Image 621 – Parâmetros: usando proxy.

Use Proxy

- Proxy name/address;
- Proxy authentication;
- User and password used to authenticate to the proxy.

41.6. E-mail classification

The **“E-mail Classification”** menu verifies specific messages. This option allows to past a source code of a specific e-mail message so Aker Spam Meter can classify it.

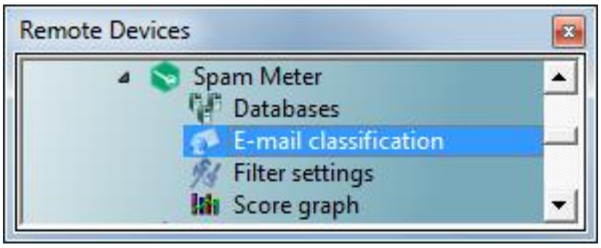
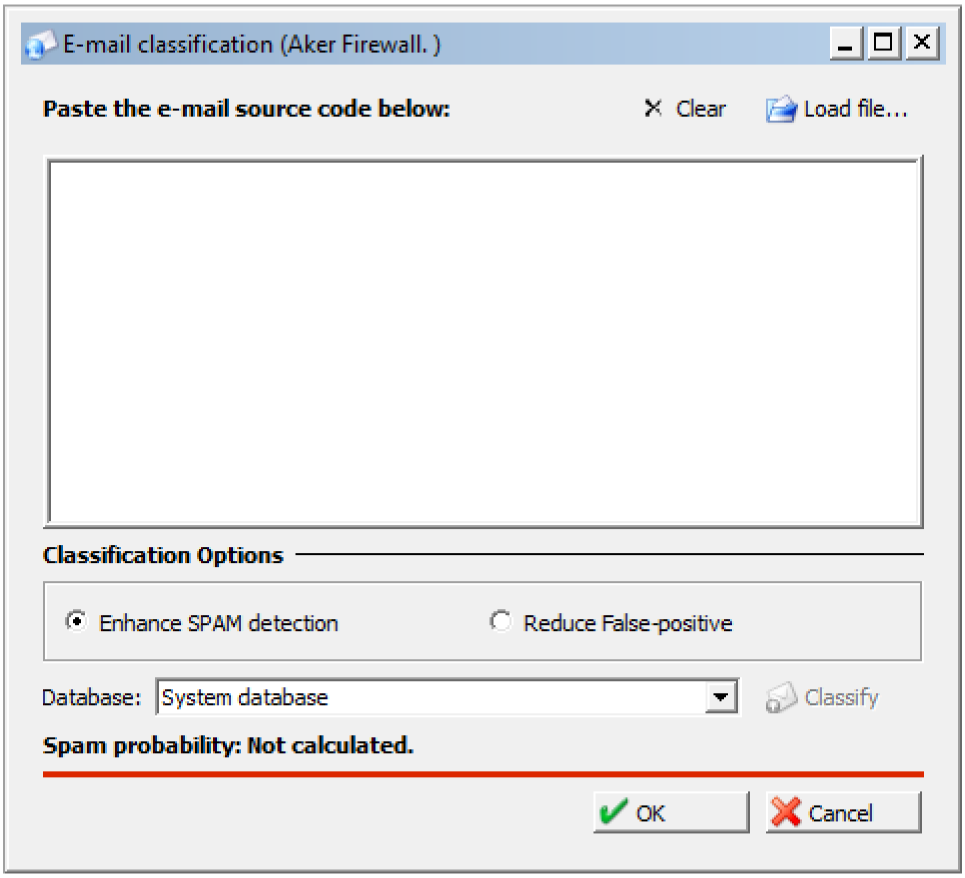

Remote Devices
Spam Meter
Databases
E-mail classification
Filter settings
Score graph

Image 622 – Access window: E-mail classification.

This way, the product’s administrator will see what punctuation Aker Spam Meter has given to the message.


E-mail classification (Aker Firewall.)
Paste the e-mail source code below:
Clear
Load file…
Classification Options
Classify
OK
Cancel

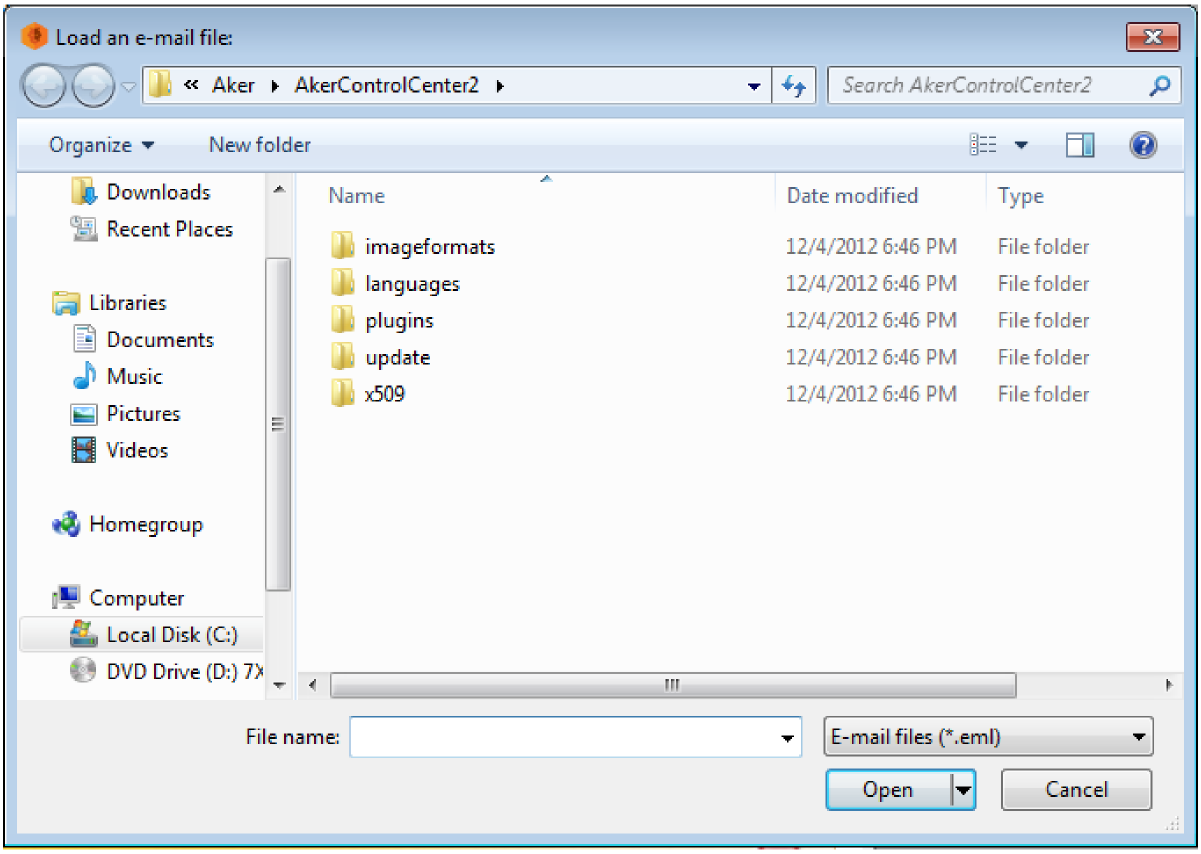
● Enhance SPAM detection ○ Reduce False-positive

Database: System database

Spam probability: Not calculated.

Image 623 – E-mail classification.

- **Clear**: Clears the text box where the email source code is typed;
- **Load File:** This option opens a window where e-mail file (*.eml) that contains the source code:


Load an e-mail file:
« Aker ▸ AkerControlCenter2 ▸
Search AkerControlCenter2
Organize
New folder
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
DVD Drive (D:) 7X
Open
Cancel

Name	Date modified	Type
imageformats	12/4/2012 6:46 PM	File folder
languages	12/4/2012 6:46 PM	File folder
plugins	12/4/2012 6:46 PM	File folder
update	12/4/2012 6:46 PM	File folder
x509	12/4/2012 6:46 PM	File folder

File name:

E-mail files (*.eml)

Image 624 – Load an e-mail file.

Classification options:

- **Enhance Spam detection**: Uses less tokens, providing a faster classification, but increasing the number of false-positives;
- **Reduce false-positive:** Uses a greater number of tokens, providing a more accurate classification, but making the process a little slow;
- **Database:** Selects which tokens' database will be used in the email classification.

41.7. Filter settings

The **“filter settings”** menu deals with the general options of storage and access to Aker Spam Meter.

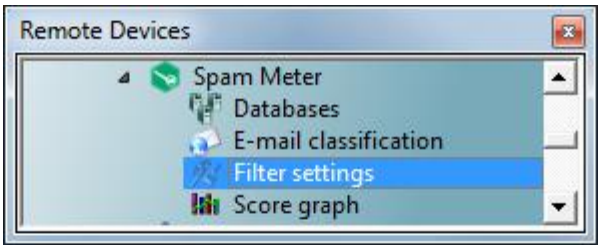
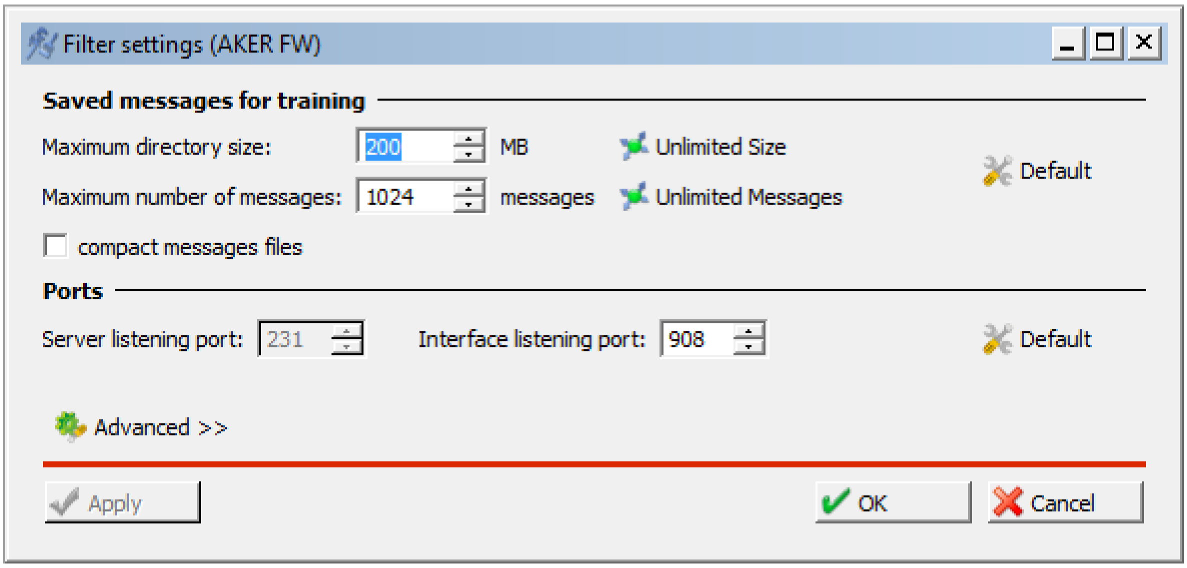

Remote Devices
Spam Meter
Databases
E-mail classification
Filter settings
Score graph

Image 625 – Access window: Filter settings.

Below follows the **“Filter settings”** window:


Filter settings (AKER FW)
Saved messages for training
Unlimited Size
Unlimited Messages
Default
Ports
Default
Advanced >>
Apply
OK
Cancel

Maximum directory size: 200 MB

Maximum number of messages: 1024 messages

☐ compact messages files

Server listening port: 231

Interface listening port: 908

Image 626 – Saved messages for training.

Saved messages for training

- **Maximum directory size:** The directory maximum size (in MB), where the email classification information will be stored.

  When using the Linux platform the command **"du -sh"** does not calculate the size of each file, it only calculates the size of the Hard Drive block, varying according to the Hard Drive that has been formatted. In a Hard drive that has been formatted to have blocks of 4KB (4096 bytes) can be seen in the following way:

- Configuration to limit the maximum number of messages in 1 MB (1024KB);
- In the directory, 1024 files of 1024 bytes each.

- Maximum directory size is 4 MB not 1 MB as expected.

Each file of 1024 bytes is physically consuming 4KB of disk which is the size of each block. This way each file of 1024 bytes is "*accounted*" as 4096 bytes on the command **"du –sh"**.

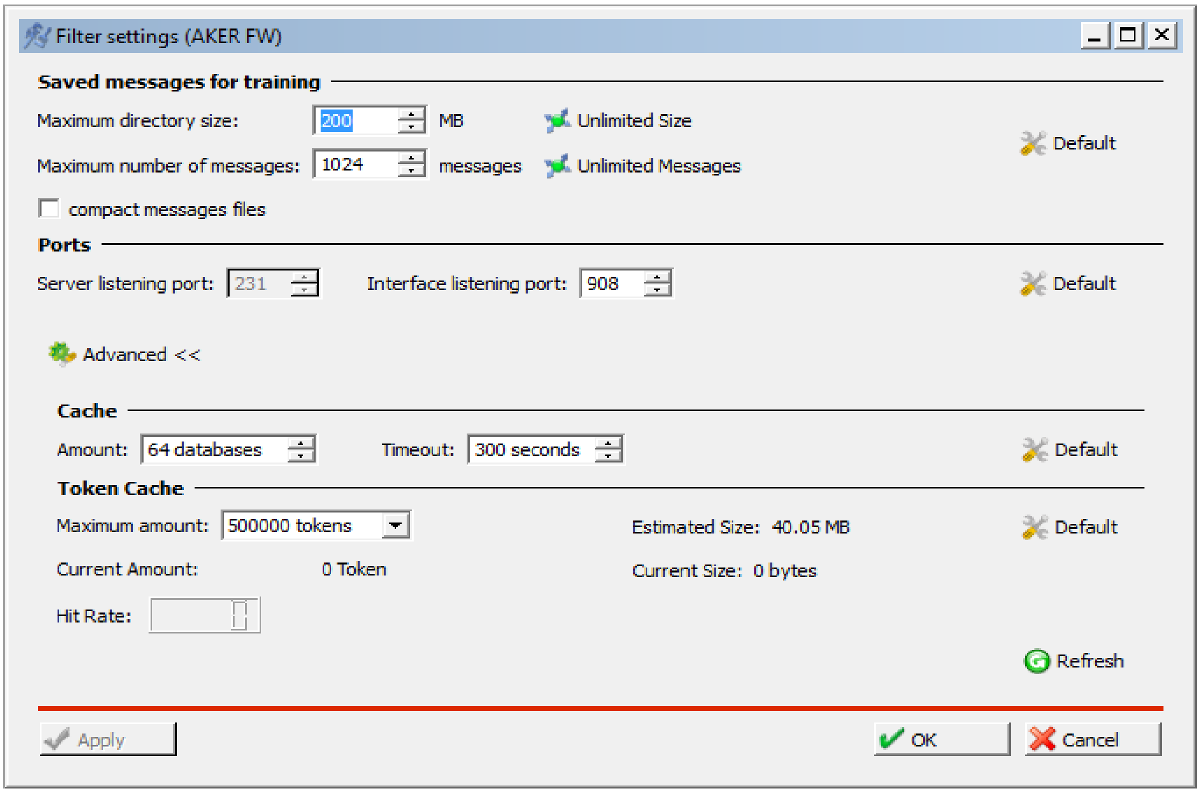
Remembering that it happens only on Unix systems, on Windows is not possible since the size is *accounted* as expected.

- **Maximum number of messages**: Maximum number of messages that will be stored.

Ports

- **Server listening port:** Indicates Aker Spam Meter server listening port that receives and classify the e-mails;
- **Interface listening port:** It is the port responsible to accept the connections directed to Aker Control Center will be allowed to connect to Aker Spam Meter.

Clicking on the "Advanced" option the following options will be enabled as displayed in the image below:



Filter settings (AKER FW)

Saved messages for training

Maximum directory size: 200 MB

Maximum number of messages: 1024 messages

☐ compact messages files

Ports

Server listening port: 231

Interface listening port: 908

Cache

Amount: 64 databases

Timeout: 300 seconds

Token Cache

Maximum amount: 500000 tokens

Estimated Size: 40.05 MB

Current Amount: 0 Token

Current Size: 0 bytes

Hit Rate:

Image 627 – Advanced Filter Settings.

Cache

- **Amount:** Database size and amount that will be allowed to be stored in the memory in order to optimize the *Product performance* ;
- **Timeout:** Time which the message will be kept in the cache in case it is not being used by the product. In case the database remains in the cache for the time set by timeout and has not been consulted, it will be removed from the volatile memory, remaining only in the disk.

Token Cache

- **Maximum amount**: Configures the server maximum amount of Token Cache;
- **Estimated Size**: Informs the Token Cache estimated size that will be occupied in the server RAM memory.
- **Current Amount**: Informs the current amount of tokens in the cache server.
- **Current Size**: Informs the Token Cache current size that will be occupied in the server RAM memory.
- **Hit Rate**: Informs the percentage of tokens that have been found in the cache during the email classification. This value tends to 100% as time passes by.

The **"Default"** icon returns the tokens maximum amount to 500000 token, which is the default setting.

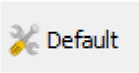


Image 628 – Default button.

The **"Refresh"** button updates the server information referring to the current amount of tokens, calculating current size and indicating the Hit rate of emails classification.

Image 629 – Refresh button.

Note: It is possible to update the URL database manually, to perform this action follow the steps below:

1. Download the file at www.aker.com.br;
2. Transfer the file to the appliance via SFTP ;
3. Open the appliance via SSH (Text Interface)
4. Execute the command: Aker> asmbase

Usage: asmbase <base_file>

Press <enter> to continue...

41.8. Score graph

Score graph presents information about the amount of e-mails that have been received/analyzed by Aker Spam Meter and their classification. Its menu is very simple, giving the administrator better idea about the emails your company has been receiving.

To gain access to the Score graph window, follow the steps below:

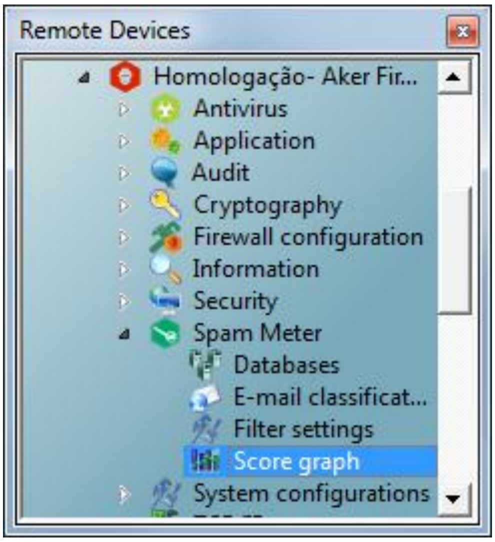

Remote Devices
Homologação- Aker Fir...
Antivirus
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter
Databases
E-mail classificat...
Filter settings
Score graph
System configurations

Image 630 – Score Graph

- Select the *Spam Meter* menu
- Click on *Score graph*:

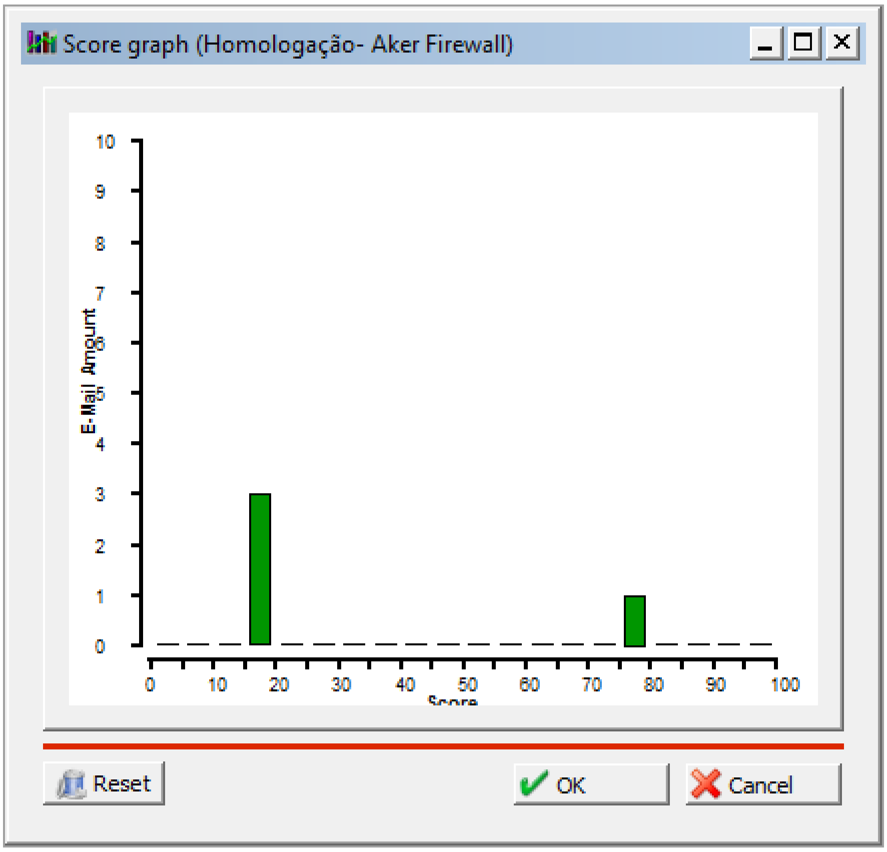

Score graph (Homologação- Aker Firewall)
E-Mail Amount
10
9
8
7
6
5
4
3
2
1
0
0
10
20
30
40
50
60
70
80
90
100
Score
Reset
OK
Cancel

Image 631 – Score graph.

41.9. Plugins

Aker Spam Meter has plugins for some email clients. These plugins allow the client to classify manually his e-mails as spam or not spam.

Aker Spam Meter has the following email clients:

- Microsoft Outlook;
- Mozilla Thunderbird.

This way, when client receives an email, he will be able to see its classification according to Aker Spam Meter Bayesian analysis.

Aker Antivirus Module

42. Aker Antivirus Module – AKAV

This chapter shows how to use AKAV on Aker Firewall.

42.1. Introduction

There are thousands of different virus and malicious software that can damage your computer and network due to it antivirus solutions must to be essential part of all information security projects. There are many types of malicious software, below follow a description of the most popular ones:

- **Virus** – A computer virus is a computer program that can replicate itself and spread from one computer to another. The term "virus" is also commonly, but erroneously, used to refer to other types of malware, including but not limited to adware and spyware programs that do not have a reproductive ability.

  Malware includes computer viruses, computer worms, Trojan horses, most rootkits, spyware, dishonest adware and other malicious or unwanted software, including true viruses. Viruses are sometimes confused with worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that appears harmless but hides malicious functions. Worms and Trojan horses, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or simply do nothing. Some viruses do nothing beyond reproducing themselves.

- **Worm** – A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

- **Hoax –** is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know. Most hoaxes are sensational in nature and easily identified by the fact that they indicate that the virus will do nearly impossible things, like blow up the recipient's computer and set it on fire, or less sensationally, delete everything on the user's computer. They often include fake announcements claimed to originate from reputable computer organizations together with mainstream news media. These bogus sources are quoted in order to give the hoax more credibility. Typically, the warnings use emotive language, stress the urgent nature of the threat and encourage readers to forward the message to other people as soon as possible.

- **Trojan horse, or Trojan** – is a type of malware that masquerades as a legitimate file or helpful program but whose real purpose is, for example, to grant a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems. Trojans may use drive-by downloads or install via online games or internet-driven applications in order to reach target computers. The term is derived from the Trojan Horse story in Greek mythology because Trojan horses employ a form of “social engineering,” presenting themselves as harmless, useful gifts, in order to persuade victims to install them on their computers.

Trojan horses in this way may require interaction with a hacker to fulfill their purpose, though the hacker does not have to be the individual responsible for distributing the Trojan horse. It is possible for individual hackers to scan computers on a network using a port scanner in the hope of finding one with a malicious Trojan horse installed, which the hacker can then use to control the target computer.

- **Security vulnerability**- Security holes/bugs are faults, defects, or programming errors. These may be exploited by unauthorized users to access computer networks or web servers from the Internet.

42.2. Introducing the appliance

The internet fraud attempts, in 2011 have grown 30% compared to 2010. The attacks caused by viruses have grown 53% in the same period. It shows that all companies connected to the internet need antivirus system acting within their network, eliminating viruses before they reach the internal servers.

Even a company that already has a corporate antivirus system installed in the internal servers and in the users machines can become overloaded in a virus outbreak, reinforcing the need of having dedicated machines for the disinfection of messages and files downloaded from the internet.

Aker Antivirus Module is a powerful appliance that makes Aker Firewall, Aker Web Gateway and Aker Secure Mail Gateway even safer. A single machine can be installed in the network and be used by several firewalls and gateways at the same time.

The appliance can be updated the virus signature files automatically, daily or even hourly, keeping it always updated. The administrator can also update the appliance whenever he wishes.

42.3. Main features

Aker Antivirus Module is an antivirus for gateways that integrates natively to Aker Firewall, Aker Web Gateway and to Aker Secure Mail Gateway enabling the disinfection of email and files downloads via WEB before they be sent to machines or internal servers.

Below follows the main features:

- Antivirus engine and signature database, automatic or daily update;
- Update schedule;
- Spyware, Trojan-horse, virus and hacking tools filtering;
- Heuristic detection of unknown virus;
- Automatic integration to Aker Firewall, Aker Web Gateway and Aker Secure Mail Gateway;
- Managed by Aker Control Center;
- Detailed log of malicious virus and programs that has been found;

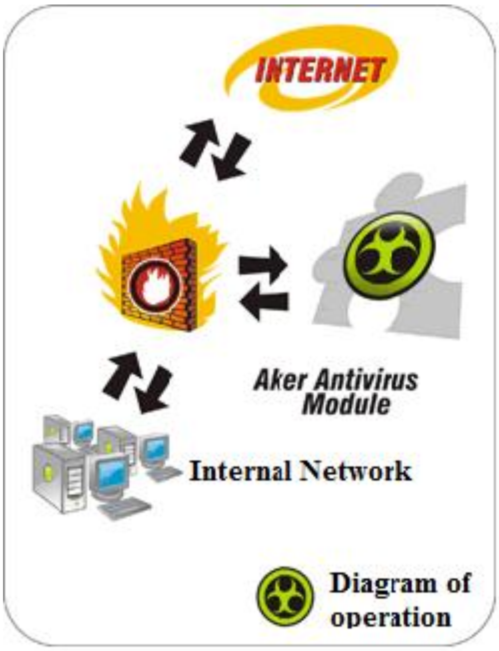


Image 633 – Aker Antivirus Module: Diagram of operation.

42.4. Aker Antivirus Module

Aker Antivirus Module is installed together with other products (Aker Firewall or any other product of Aker), inheriting functions such as *user administration, log's view, updates, etc*. The picture below describes its functioning:

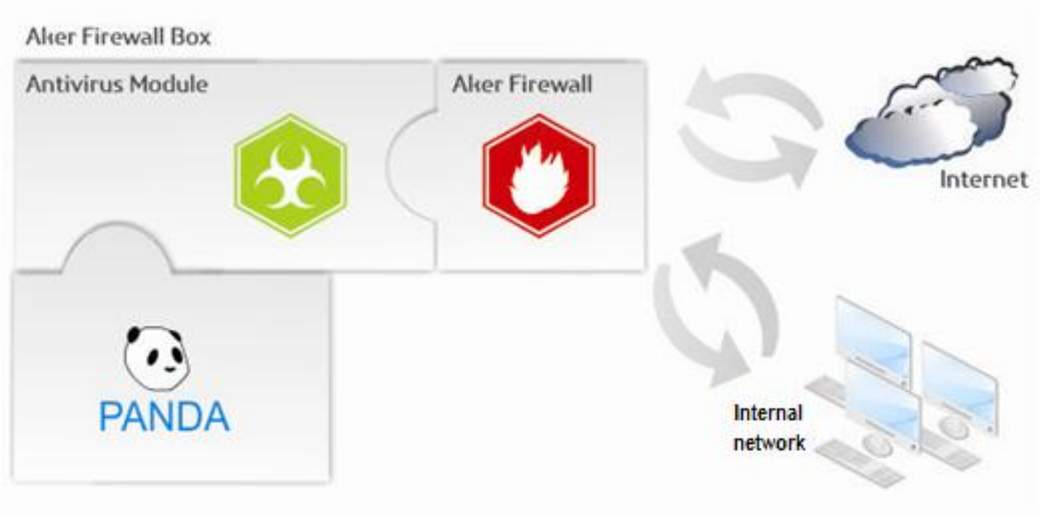


Image 635 – Diagram of operation 3.

When user is making a download for the first time through a local network, Aker Firewall will establish connection with **Aker Antivirus Module**, sending the files to it, so these files can be analyzed, verifying if they are infected or not. Once these files have been analyzed, **Aker Antivirus Module** will communicate to the Firewall which files will be accepted and which will be blocked, informing the user who is attempting to download these files.

42.5. Configuring Aker Antivirus Modulo

Aker Antivirus Module is remotely managed through Aker Control Center, which is a Remote Interface that controls all solutions of Aker. Aker Antivirus Module provides an interface for partners. These partners are provided by third parties. Aker's recently partner is PANDA.

Once the product license is acquired the user will have access to partner.

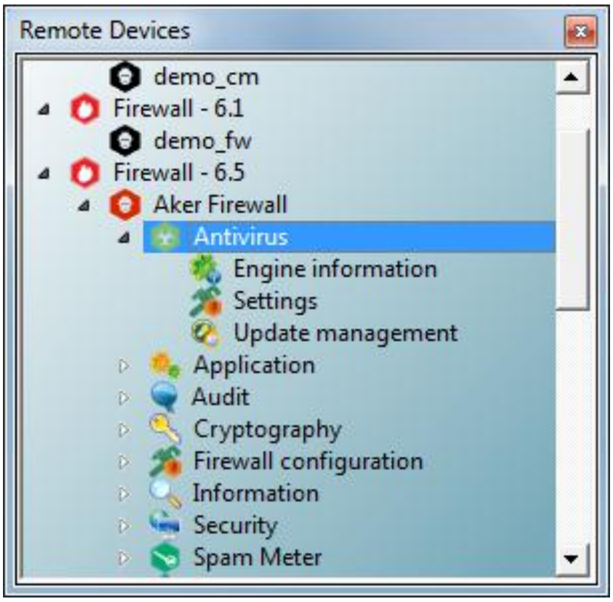

Remote Devices
demo_cm
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Engine information
Settings
Update management
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter

Image 636 – Antivirus

42.6. Settings

To gain access to the *Antivirus* window follow the steps below:

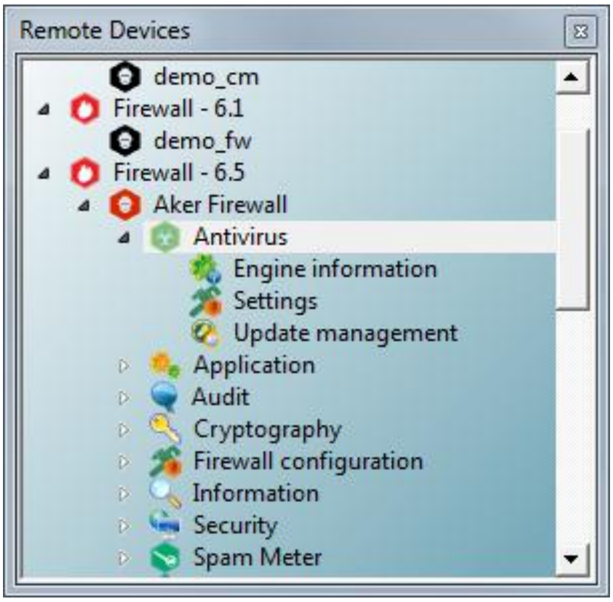

Remote Devices
demo_cm
Firewall - 6.1
demo_fw
Firewall - 6.5
Aker Firewall
Antivirus
Engine information
Settings
Update management
Application
Audit
Cryptography
Firewall configuration
Information
Security
Spam Meter

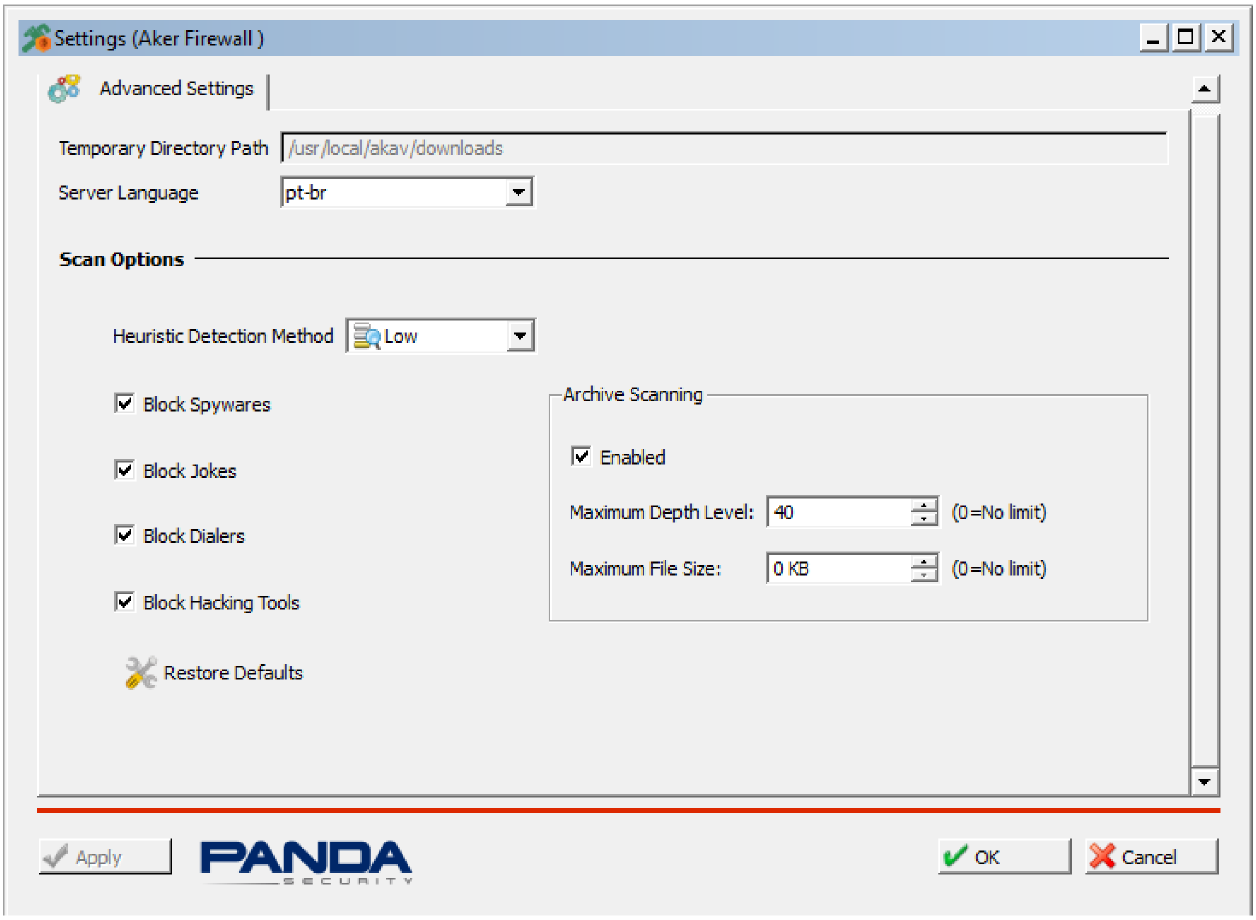
Image 637 – Aker Antivirus

- Open the remote device you wish to use
- Select *Antivirus*.

Settings window

This window has specific configuration options of the Partner which is being used. Each Partner has its own resource and options of the product, virus scan options vary from partner to partner.

Advanced Settings tab


Settings (Aker Firewall)
Advanced Settings
Restore Defaults
Apply
PANDA SECURITY
OK
Cancel

Temporary Directory Path: /usr/local/akav/downloads

Server Language: pt-br

Scan Options

Heuristic Detection Method: Low

☑ Block Spywares

☑ Block Jokes

☑ Block Dialers

☑ Block Hacking Tools

Archive Scanning

☑ Enabled

Maximum Depth Level: 40 (0=No limit)

Maximum File Size: 0 KB (0=No limit)

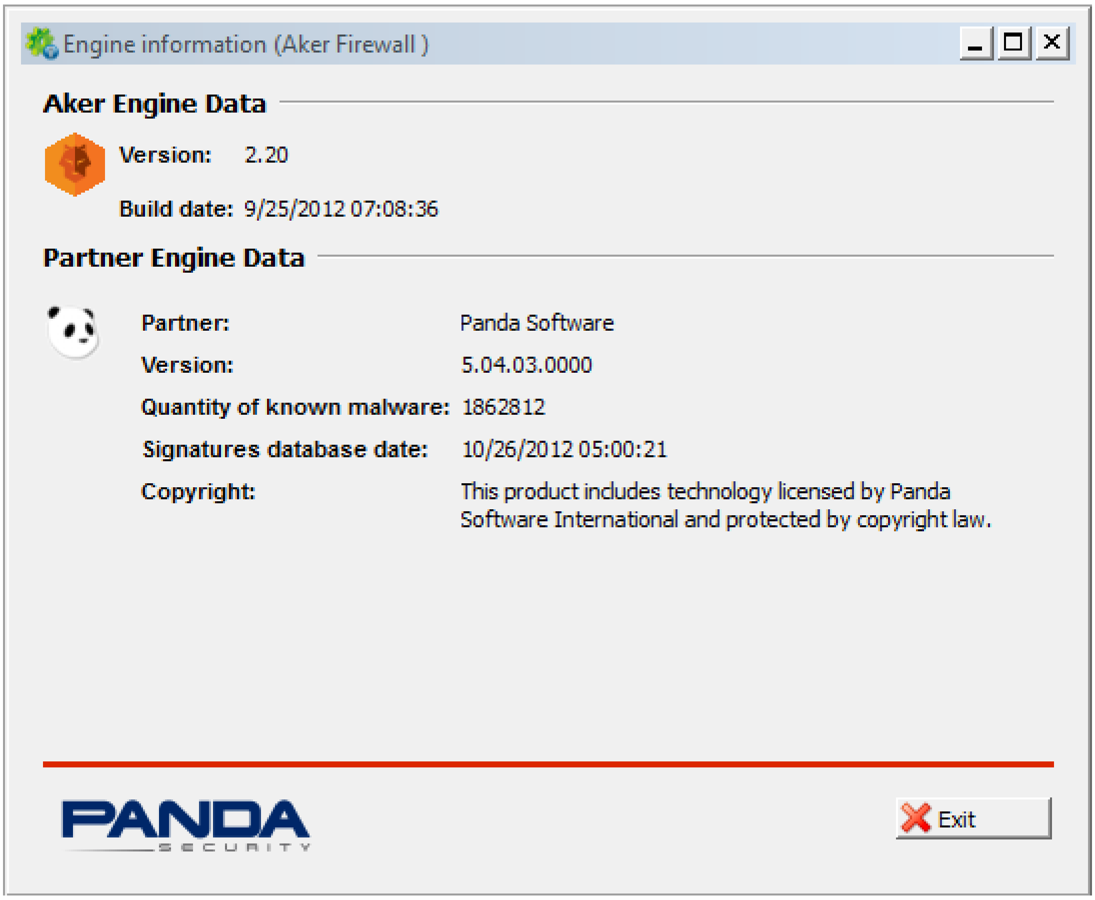
Image 638 – Advanced Settings.

Below follow the description of the option in the **Settings** window:

- **Temporary Directory Path:** Place where Aker Antivirus Module will store the files that will be scanned.
- **Server Language:** Selects the language that the server will generate the logs, the available options are: **"pt-br"** and **"en-us"**;
- **Scan Options:** Configures the scan options used by the Partner (PANDA)

42.7. Engine information

This window presents Aker and its Partner engine data information.



Engine information (Aker Firewall)

Aker Engine Data

Version: 2.20

Build date: 9/25/2012 07:08:36

Partner Engine Data

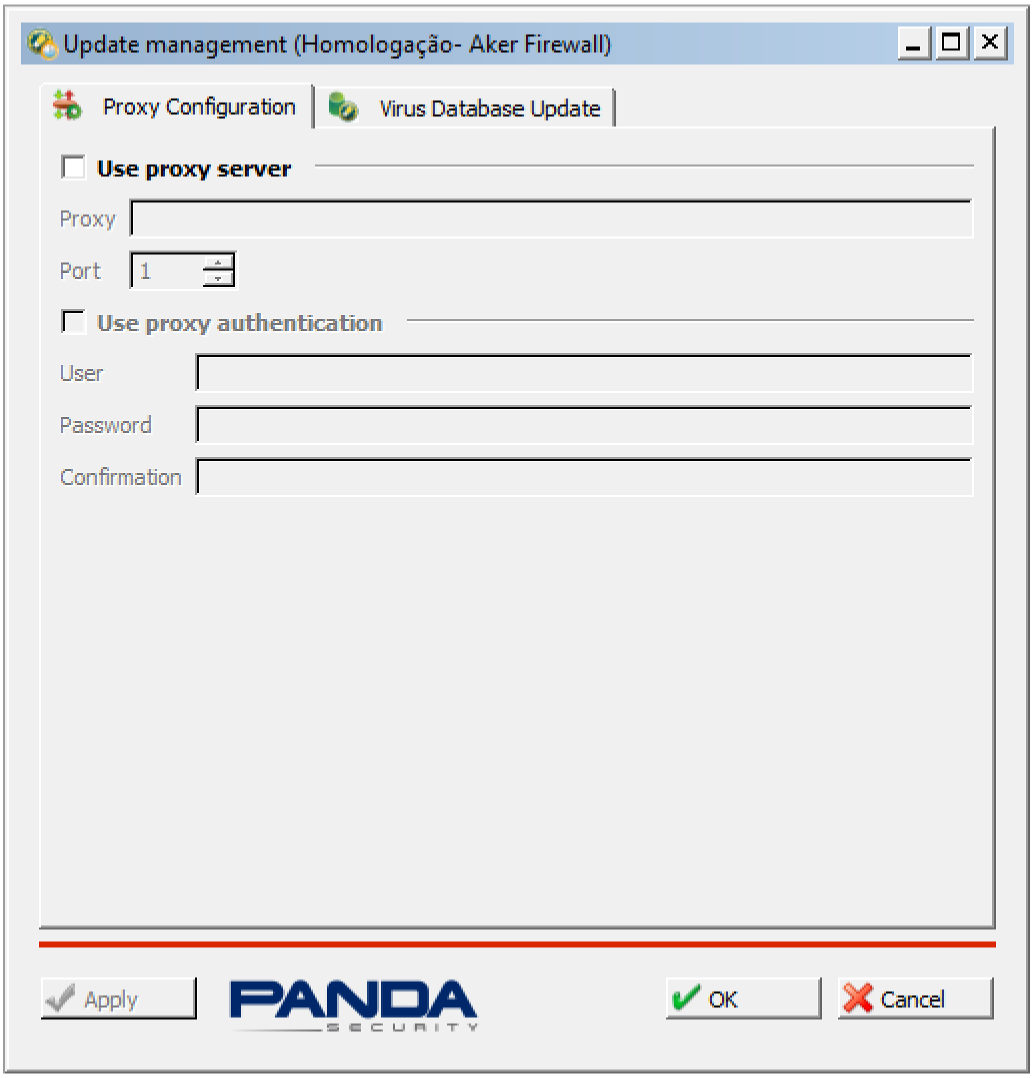
Partner:	Panda Software
Version:	5.04.03.0000
Quantity of known malware:	1862812
Signatures database date:	10/26/2012 05:00:21
Copyright:	This product includes technology licensed by Panda Software International and protected by copyright law.

PANDA SECURITY
Exit

Image 639 – Aker Engine Data

42.8. Update management

In this window configures how the updates will be performed. It consists of two tabs: *Proxy Configuration and Virus Database Update*. The description of these tabs follow below:

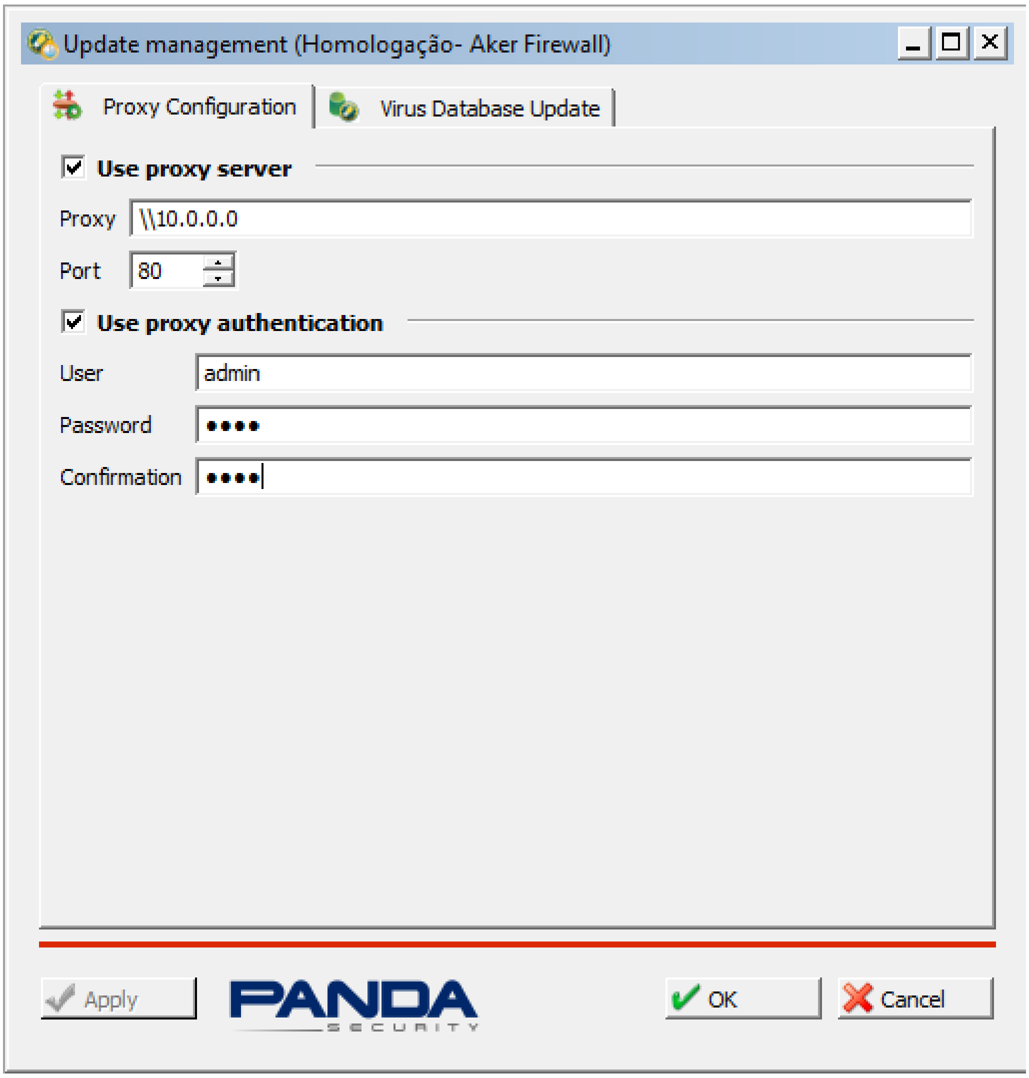


Update management (Homologação- Aker Firewall)
Proxy Configuration
Virus Database Update
☐ Use proxy server
Proxy
Port
☐ Use proxy authentication
User
Password
Confirmation
Apply
PANDA SECURITY
OK
Cancel

Port: 1

Image 640 – Update management.

Proxy Configuration tab


Update management (Homologação- Aker Firewall)
Proxy Configuration
Virus Database Update
Apply
PANDA SECURITY
OK
Cancel

☑ **Use proxy server**

Proxy: \\10.0.0.0

Port: 80

☑ **Use proxy authentication**

User: admin

Password: ••••

Confirmation: ••••

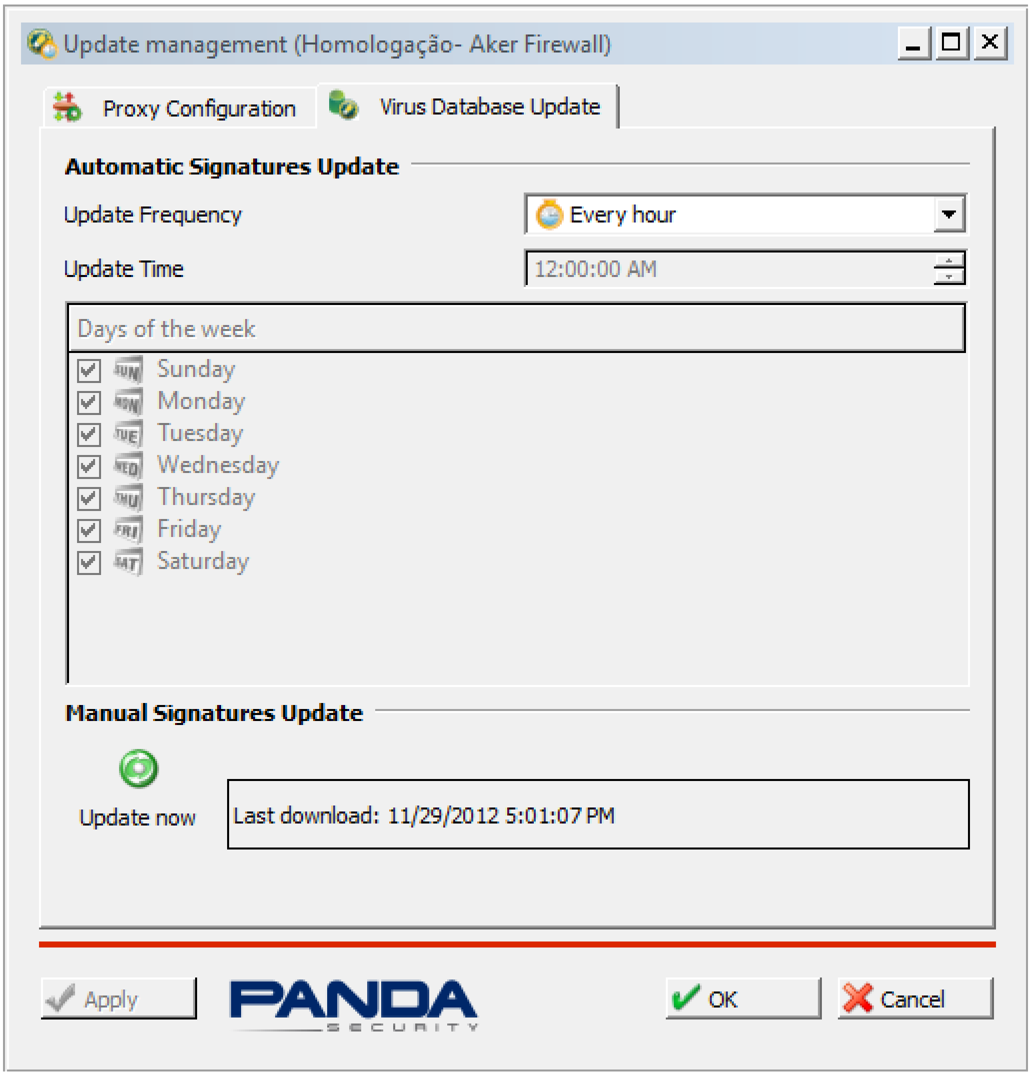
Image 641 – Update management (Proxy configuration)

The signature update is made through the Internet. In case user needs to authenticate in a proxy to connect to the Internet, this configuration will be set in this window.

- **Use proxy server** – the following options will be available only if this option is enabled.
  - **Proxy:** Server IP address.
  - **Port:** Port that will be used in this operation.

- **User proxy authentication:** Enabling this option user will be able to authenticate to proxy, registering username and password:
  - **User:** Username that will authenticate to proxy;
  - **Password:** Password that will be used to authenticate to proxy;
  - **Confirmation:** Retype your password

Virus Database Update



Update management (Homologação- Aker Firewall)

Automatic Signatures Update

Update Frequency: Every hour

Update Time: 12:00:00 AM

Days of the week

☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Manual Signatures Update

Last download: 11/29/2012 5:01:07 PM

Image 642 – Update management (Virus database Update)

In this tab the user can update the Virus database, or set day and time to perform the update automatically.

- **Update frequency:** Sets how the update will be automatically performed, the options are :
  - **Specific days:** Selects weekday and time that the automatically update will be performed;
  - **Every hour:** Selecting this option the update will be performed hourly;
- **Update Time:** Sets the time that the updates will be performed.
- **Days of the week:** Sets the days of the week that the update will be performed.
- **Update now:** Updates the v1irus database immediately.

Appendix A – System messages

43. Appendix B – Copyrights e Disclaimers

In this appendix the disclaimers of the libraries and third party source codes used in Aker Firewall are listed. These disclaimers apply only to the explicit mentioned parts and not to Aker Firewall as a whole. They are mentioned here due to requirements of the developers.

DES Library

Copyright (C) 1995 Eric Young (eay@mincom.oz.au)
All rights reserved.

This library and applications are
FREE FOR COMMERCIAL AND NON-COMMERCIAL USE
as long as the following conditions are aheared to.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed. If this code is used in a product,
Eric Young should be given attribution as the author of the parts used.
This can be in the form of a textual message at program startup or
in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by Eric Young (eay@mincom.oz.au)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS
OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence
[including the GNU Public Licence.]

libcrypto Encryption Library

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written
by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The license and distribution terms for any publically available version or
derivative of this code cannot be changed. i.e. this code cannot simply be
copied and put under another distribution license
[including the GNU Public License.]

SNMP Library

Copyright 1997 by Carnegie Mellon University
All Rights Reserved
Permission to use, copy, modify, and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU not be
used in advertising or publicity pertaining to distribution of the
software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE,
INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS,
IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR
CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

FreeBSD source codes

Copyright (c) 1982, 1986, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions
and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions
and the following disclaimer in the documentation and/or other materials provided with the
distribution.
3. All advertising materials mentioning features or use of this software must display the following
acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or
promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS''
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MD5 Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data
Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or

referencing this
software or this function.

License is also granted to make and use derivative works provided that such works
are identified
as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all
material
mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the
merchantability of this
software or the suitability of this software for any particular purpose. It is provided "as
is" without
express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation
and/or software.

SNMP Agent

Copyright (c) 1996,1997 Wes Hardaker and the University of California at Davis

COPYRIGHT

Many portions of the code in this package were distributed by Carnegie Mellon
University.
All other code and changes to the original code written by Wes Hardaker at the
University of
California at Davis is copyrighted under the following copyright:

Permission is granted to use, copy, modify and distribute this software and
documentation. This
software is distributed freely and usage of it is not subject to fees of any kind. It may
be included in
a software compact disk set provided that the author is contacted and made aware
of its
distribution.

LInteger math library

LInteger Version 0.2 Source Code and Documentation

Copyright (C) 1996 by Leonard Janke

This source code and documentation may be used without charge for both
commercial and non-commercial use. Modification of the source code or
documentation is allowed provided any derivate work is clearly indentified as such
and all copyright notices are retained unmodified. Redistribution of the source code
or documentation is unlimited, except by the limits already mentioned, provided that
the redistribution is not for profit. Those wishing to redistribute this source code or

documentation or any work derived from either for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone who wishes to distribute a program statically linked against the functions provided may do so providing that he or she includes a copy of this note with the program.

Distribution of libraries compiled from this source code is unlimited if the distribution is not for profit and this copyright notice is included. Those wishing to distribute libraries compiled from this source code or any work derived from it for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone using this source code or documentation or any work derived from it, including, but not limited to, libraries and statically linked executables, must do so at his or her own risk, and with understanding that Leonard Janke will not be held responsible for any damages or losses that may result.